

2

NAVAL POSTGRADUATE SCHOOL

Monterey, California

DTIC
ELECTE
AUG 14 1991
S D D



AD-A239 431



THESIS

IDENTIFYING SECURITY PROBLEMS AND DEVISING
CONTROL SOLUTIONS IN A LOCAL AREA NETWORK:
A CASE STUDY APPROACH

by

Gary John Evans

September 1990

Thesis Advisor:

Tung Xuan Bui

Approved for public release; distribution is unlimited

91-07720



91 13 035

**Best
Available
Copy**

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b. RESTRICTIVE MARKINGS	
2a. SECURITY CLASSIFICATION AUTHORITY			3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited	
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE				
4. PERFORMING ORGANIZATION REPORT NUMBER(S)			5. MONITORING ORGANIZATION REPORT NUMBER(S)	
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School		6b. OFFICE SYMBOL (If applicable) Code 37		7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000			7c. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000	
8a. NAME OF FUNDING/SPONSORING ORGANIZATION		8b. OFFICE SYMBOL (If applicable)		9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)			10. SOURCE OF FUNDING NUMBERS	
			PROGRAM ELEMENT NO	PROJECT NO
			TASK NO	WORK UNIT ACCESSION NO.
11. TITLE (Include Security Classification) IDENTIFYING SECURITY PROBLEMS AND DEVISING CONTROL SOLUTIONS IN A LOCAL AREA NETWORK: A CASE STUDY APPROACH				
12. PERSONAL AUTHOR(S) Evans, Gary J.				
13a. TYPE OF REPORT Master's Thesis		13b. TIME COVERED FROM _____ TO _____		14. DATE OF REPORT (Year, Month, Day) 1990, September
15. PAGE COUNT 98				
16. SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)	
FIELD	GROUP	SUB-GROUP	Computer Security; Local Area Network (LAN); Security and Control	
19. ABSTRACT (Continue on reverse if necessary and identify by block number) This thesis investigates the requirements for establishing security criteria in designing and developing a local area network (LAN) for an aviation squadron. In particular, it concentrates on the security problems and control issues in the design of a LAN. A survey of the security literature on computer security was conducted to develop a model for identifying security problems in a local area network and devise control solutions. A case study was written based on the literature review and previous experience in the aviation community. Although many controls solutions are discussed, adequate planning, common sense and proper user training all play an integral part in developing an atmosphere of security awareness in networks.				
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS PRT <input type="checkbox"/> DTIC USERS			21. ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a. NAME OF RESPONSIBLE INDIVIDUAL Prof. Tung Bui			22b. TELEPHONE (include Area Code) (408) 646-2630	22c. OFFICE SYMBOL Code AS/BC

Approved for public release; distribution is unlimited

Identifying Security Problems and Devising Control
Solutions in a Local Area Network: A Case Study Approach

by

Gary John Evans
Lieutenant Commander, United States Navy
B.S., United States Naval Academy, 1978

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

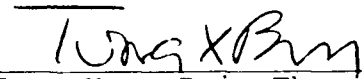
from the


NAVAL POSTGRADUATE SCHOOL
September 1990

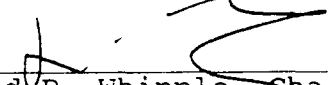
Author:


Gary J. Evans

Approved by:


Tung Xuan Bui, Thesis Advisor


Henry H. Smith, Second Reader


David R. Whipple, Chairman,
Department of Administrative Sciences

ABSTRACT

This thesis investigates the requirements for establishing security criteria in designing and developing a local area network (LAN) for an aviation squadron. In particular, it concentrates on the security problems and control issues in the design of a LAN. A survey of the security literature on computer security was conducted to develop a model for identifying security problems in a local area network and devise control solutions. A case study was written based on the literature review and previous experience in the aviation community. Although many controls solutions are discussed, adequate planning, common sense and proper user training all play an integral part in developing an atmosphere of security awareness in networks.



ACCOMPLISHED FOR	
NTIS COPY	J
DATE	
BY	
JANUARY 1981	
By	
L. H. BROWN	
F. H. BROWN	
DR	AND OTHER
A-1	

TABLE OF CONTENTS

I.	INTRODUCTION -----	1
	A. BACKGROUND -----	1
	B. OBJECTIVES -----	2
	C. THE RESEARCH QUESTION -----	3
	D. SCOPE AND LIMITATIONS -----	3
	E. RESEARCH METHODOLOGY -----	3
	F. ORGANIZATION OF THE STUDY -----	4
II.	A CASE STUDY APPROACH TO ADDRESS SECURITY PROBLEMS IN LANS -----	5
	A. INTRODUCTION -----	5
	B. A CASE STUDY FOR A NAVY AVIATION SQUADRON --	5
	C. A CASE STUDY: LAN PATROL -----	7
	D. TEACHING GUIDE -----	17
III.	BASIC LAN TERMINOLOGY -----	19
	A. INTRODUCTION -----	19
	B. LAN ARCHITECTURE -----	20
	C. TOPOLOGY AND ACCESS PROCEDURES -----	22
	D. TRANSMISSION MEDIA -----	25
	E. LAN STANDARDS OVERVIEW -----	29
	F. COMPARISON OF LOCAL AREA NETWORKS -----	29
	G. SUMMARY -----	30

IV.	CLASSIFICATION OF SECURITY PROBLEMS IN LANS ----	31
A.	INTRODUCTION -----	31
B.	SECURITY -----	33
C.	SUMMARY -----	47
V.	CLASSIFICATION OF CONTROL SOLUTIONS FOR LANS ---	48
A.	INTRODUCTION -----	48
B.	PHYSICAL ACCESS -----	51
C.	RECOVERY CONTROLS -----	62
D.	DATA SECURITY CONTROL -----	66
E.	COMMUNICATION -----	71
F.	CABLING AND ELECTRICAL DESIGN -----	72
G.	MANAGEMENT CONTROLS -----	74
H.	THE USER -----	77
I.	SUMMARY -----	80
VI.	RECOMMENDATIONS, CONCLUSIONS, AND SUGGESTIONS FOR FUTURE RESEARCH -----	82
A.	SUMMARY OF RESULTS -----	82
B.	RECOMMENDED SOLUTIONS FOR THE PROPOSED CASE STUDY -----	83
C.	SUGGESTIONS FOR FUTURE RESEARCH -----	85
	LIST OF REFERENCES -----	87
	INITIAL DISTRIBUTION LIST -----	91

I. INTRODUCTION

A. BACKGROUND

The 1990's will see information processed faster, cheaper and a significant increase in networking of computers. Indeed, local area networks (LANs) are becoming more popular with the proliferation of microcomputers in the work place. The reason for the local area network (LAN) popularity is described by Chorafas' statement "that the essence of the personal computer (PC) and LAN revolution is individual access at an affordable price." [Ref. 1:p. 9] As LANs have expanded in the work place, problems have developed which should have been anticipated in the design and planning phase of the project.

In this age of information technology, computer security is a basic concern in the Department of Defense (DoD) and the Department of the Navy (DoN). Microcomputer security is a relatively new arena that involves many of the old mainframe security issues plus new problem areas in microcomputers and networks.

Two important issues to consider in the design of a local area network (LAN) are security and control. Security deals with more than the protection of classified information in a LAN. Security topics for any computer system include such areas as service denial, damage, unintentional harm and

viruses. Security and control measures are equally important in an unclassified environment when dealing with sensitive or personal information. These areas will be discussed in the thesis.

The addition of more microcomputers can create highly dispersed, redundant databases and possibly inefficient use of computer hardware.

In an atmosphere of budget cuts and monetary restraint, the Navy should start to focus on establishing local area networks to share software, hardware and information. With the expansion of microcomputers in Navy aviation squadrons, it is feasible to buy local area networks and resolve this problem.

B. OBJECTIVES

The objective of this thesis is to identify security problems and control solutions in the design of local area networks. After identifying the issues and the areas to examine, a case study is presented to demonstrate the security concerns in a network environment. It can be used to raise security awareness of officers in charge of implementing LANs at Navy aviation squadrons.

The second objective is to outline security and control issues and their importance in LANs and microcomputers.

C. THE RESEARCH QUESTION

The research question is "What are the security problems and control solutions in a local area network design for an aviation squadron?" These issues should be addressed in the planning and design phase to avoid unnecessary cost for additional software and future expansion.

D. SCOPE AND LIMITATIONS

The main thrust of the thesis concentrates on the security and control issues in the design of a local area network in an unclassified environment. The issues addressed are appropriate for all aviation squadrons.

This thesis does not suggest a particular local area network architecture for a squadron or develop a cost\benefit analysis of a local area network. Both of these topics are suggested follow-on topics to this thesis.

E. RESEARCH METHODOLOGY

A literature review was conducted to compile all the security and control issues in a LAN environment. Department of Defense (DoD) and Department of the Navy (DoN) instructions on computer security and networks were included in the review.

A review of all theses completed on LANs at the Naval Postgraduate School was completed to examine the depth that previous theses researched into the security and control issues. Omission of security issues in the system design was

a primary limitation on all previous local area network theses.

A survey of the security literature was conducted to develop a model for identifying security problems in a local area network and devise control solutions. A case study was written from the literature review material.

F. ORGANIZATION OF THE STUDY

A case study is provided in Chapter II to help understand security and control issues in a patrol aviation squadron before purchasing a network. Chapter III is a general overview of LAN characteristics. Chapter IV presents classifications of security problems in a local area network. The security issues include hardware security, software security, physical security, communication security and human related security. Chapter V proposes a taxonomy of control solutions in local area networks. The control issues include but are not limited to access controls, data controls, communication controls and management controls. Chapter VI summarizes the findings of this study and formulates recommendations for future research.

II. A CASE STUDY APPROACH TO ADDRESS SECURITY PROBLEMS IN LANS

A. INTRODUCTION

The case study is designed for classroom/workshop discussion on security and control issues in computer systems and local area networks. The case study should assist students examine different problems in security when designing a local area network.

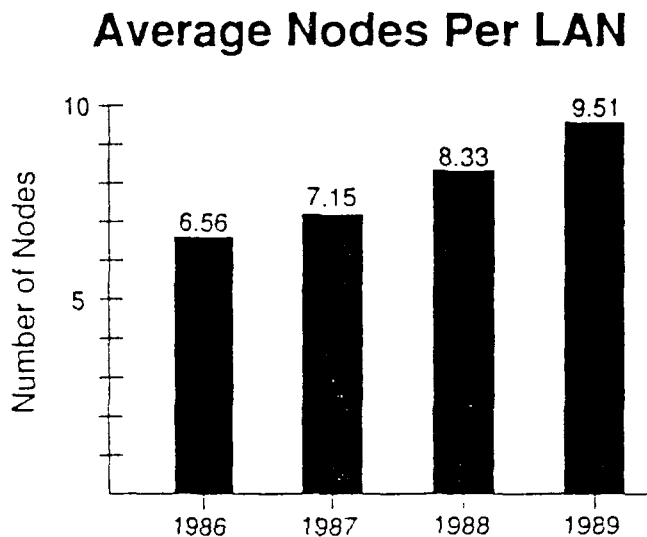
The case has the following educational objectives:

- To identify the security issues involved in a local area network.
- To develop control and management solutions to resolve the security problems.
- To enable the student to gain an appreciation of the security issues in an unclassified network environment.

B. A CASE STUDY FOR A NAVY AVIATION SQUADRON

Originally Patrol Squadron 31 was chosen as the squadron upon which to base the case. This determination was made because of the size of the command and the number of microcomputers (Zenith-248's) in the squadron. After further study it was determined to discuss a generic squadron case study instead of a specific squadron. The typical squadron has had an inventory consisting of between four to six personal computers (PCs). An International Data Corporation (IDC) report released in September 1989 stated that the

average number of microcomputers or nodes in a typical network was 9.51 in 1989. IDC forecast that the average node per LAN will be 14.35 by the end of 1993. [Ref. 2:p. 41] Figure 2.1 depicts the average nodes per LAN from 1986 to 1989.



Source: [Ref. 2:p. 42]

Figure 2.1 Average Nodes Per LAN

This case does not reflect the current or past environment in any patrol aviation squadron. Ninety percent of the information discussed in the case study is from the literature review. Personal experience from two patrol aviation commands and observations as command inspection coordinator on an overseas staff add some reality to the case.

C. A CASE STUDY: LAN PATROL

As the fog began to rise over the runway, the morning drizzle at Naval Air Station (NAS) Whidbey Island, Washington started to subside. NAS Whidbey Island is the home port of Patrol Squadron FORTY-TWO (VP-42).

VP-42 is one of five operational fleet patrol aviation (P-3C) squadrons. The primary mission of patrol aviation is to detect and track enemy submarines. The squadron is composed of approximately 40 officers and 200 enlisted personnel.

The Executive Officer (XO) of VP-42 is Commander (CDR) "Buss" Ether. CDR Ether just completed reading an article in the local newspaper on the effectiveness and capabilities of local area networks (LANs). After writing the advantages and disadvantages of a LAN on a note pad (Table 2.1), the XO decided to talk to the Commanding Officer (CO). The XO walked into the Commanding Officer's office to explain the benefits of a local area network (LAN).

The Commanding Officer is CDR "Bull" Zenith. A salty Naval Flight Officer (NFO) who has spent more time tracking submarines while in the head (bathroom) than most Lieutenants have tracking submarines for their career.

After knocking on the CO's door, the XO stepped into the office. "CO, I think it is time for this squadron to acquire a local area network."

The CO stated, "Well XO, what are the advantages of a local area network? How much will it cost?"

The XO paused and remembered from the article a few advantages. "CO, the first advantage is that we will be able to send electronic mail (E-mail) to all the departments. Another advantage is a centralized database and sharing of computer resources like the new laser printer. I have listed further advantages and some disadvantages of a LAN for you to examine."

TABLE 2.1

ADVANTAGES AND DISADVANTAGES OF A LAN

Advantages

1. Electronic mail will save time on memo's and save individuals from searching the spaces for someone.
2. Resource sharing of advance equipment.
3. Elimination of redundant databases.
4. Access to other networks.

Disadvantages

1. Games being played on the network.
 2. Possibility of viruses.
 3. Expense of maintaining network.
 4. More computer training required.
 5. Someone to manage.
 6. The current system does not require additional funds.
-

"Thanks XO." As the CO turned to his organizational chart on the wall (Figure 2.2) he stated, "OK XO, let's assign one of our new Lieutenant Commanders to review the security issues and report his findings."

XO stated, "I will put Lieutenant Commander (LCDR) Token in charge."

LCDR Token stepped out of his car and headed towards the Executive Officer's office to discuss his first job in the squadron. As LCDR "Ringer" Token stepped into the XO's office he wondered what job he was obtaining. "Good morning, XO."

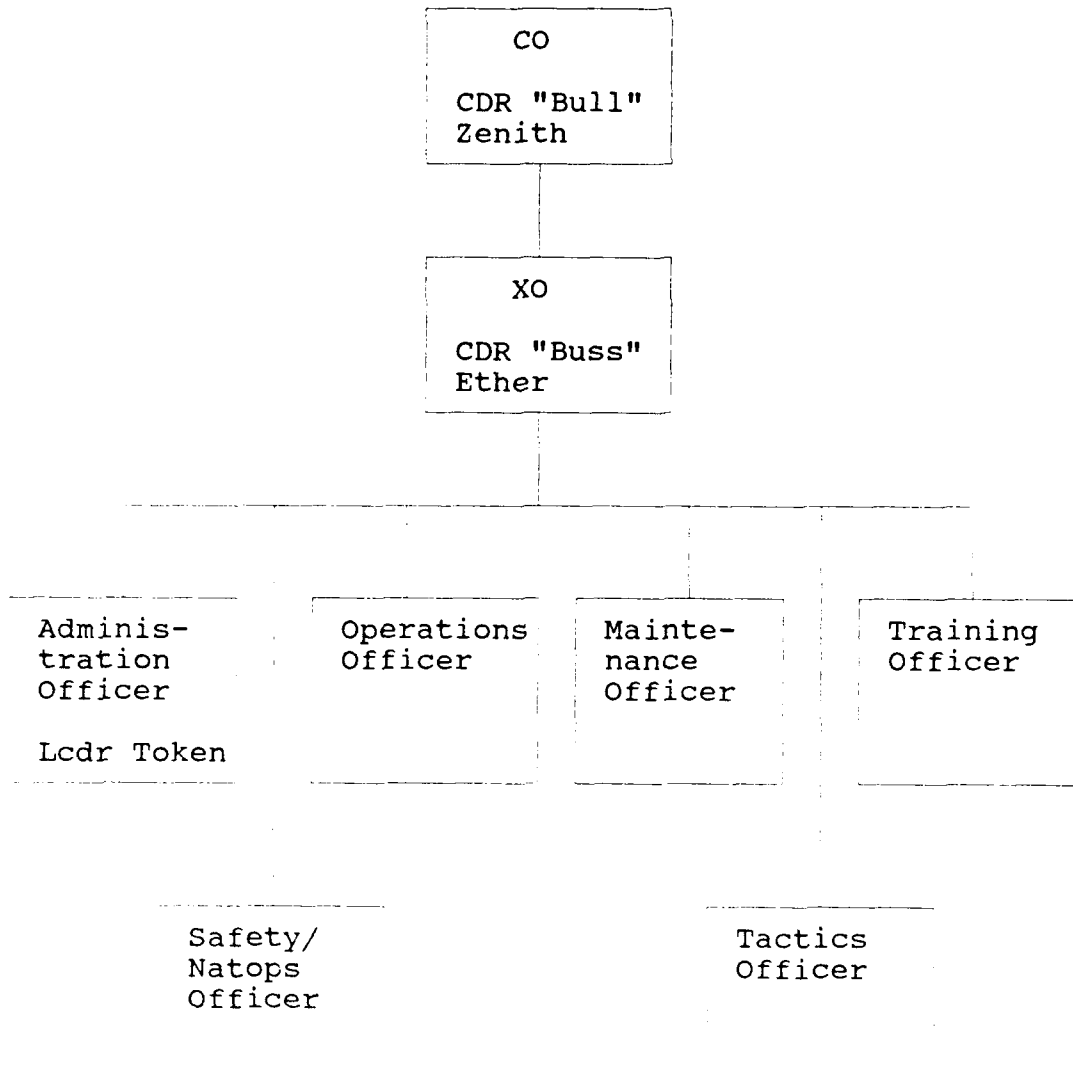


Figure 2.2 Unit Organization

"Good morning, 'Ringer'. Please sit down so I can discuss your new job. You are going to be the new Administration Officer and the CO has tasked you with a small project. The command is interested in buying a local area network (LAN). I want you to look into the security problems involved in a LAN. I believe that security in this type environment is

small so the project should be done quickly. Do some research and draft a response to the CO."

"Yes, Sir. Although I am a PC novice, this should be an interesting task."

LCDR Token started his research by finding an inventory of the personal computers in the command. The computers and locations are summarized in Table 2.2.

TABLE 2.2
COMPUTER RESOURCES AT VP-42

COMPUTER	DEPARTMENT	NUMBER	USE
Unisys-386	Administration	2	word processing, graphics
Unisys-386	Operations	1	word processing, spreadsheet
Unisys-386	Maintenance	2	word processing, spreadsheet, database
Unisys-386	Training	1	word processing
Zenith-248	Safety	1	word processing
Zenith-248	Tactics	1	word processing

LCDR Token reviewed the Automatic Data Processing (ADP) Security Manual and pertinent instructions on local area networks. He researched various computer magazines on local area networks including LAN Magazine and felt a little more comfortable about the security issues. Sitting at a computer terminal, Ringer attempted to get his ideas in order. First, he had to find his diskettes. He always had a habit of leaving the diskettes by the computer and usually unlabeled.

Since the computer was already on, he wasted no time typing in his ideas.

LCDR Token's assistant for the project was LT Joe Hacker. Joe is the computer wizard of the squadron and usually spends more time trying to sell computers to his squadron mates than actually doing his job. Joe tells LCDR Token not to worry about purchasing a virus checker because he copied a program off a reliable public bulletin board. Joe is excited about the new LAN and can not wait to copy the latest version of WordPerfect and the latest spreadsheet software.

At the weekly Tuesday department head meeting, the CO asked for suggestion on security measures to be considered for a local area network. Ideas on the subject should be given to LCDR Token by the following Friday.

CDR "Smithy" Corona is the LDO Maintenance Officer. "We don't need a LAN. We only use the computers for word processing. Sounds like this could be an expense adventure. I would rather have a couple of typewriters and a good typist."

After the meeting, "Ringer" needed a breath of fresh air.

As "Ringer" was walking back to his office, he was stopped by LCDR Bill Compaq.

Bill: "Ringer, can I talk to you for a few minutes in my office."

Ringer: "Sure."

Bill: "Ringer, I heard rumors that the local area network is going to have many security features and controls. You realize if you have too many controls nobody will use the system."

Ringer: "Bill, we are just in the design phase. I have to make a recommendation on what type of security the LAN should have to the CO. I believe that users should use the PC lock on the front of the computer and a password to enter the LAN."

Bill: "People don't use that key. Most people keep the key in the computer or hide the key so they don't lose it. Additionally, I think using passwords on an unclassified LAN is a bad idea. I have enough items to memorize now."

Ringer: "Don't worry about the password. The password will be easy to remember and each department will have the same password."

Bill: "Passwords will not work. The user will write the password down and probably post it on the computer."

Ringer: "Bill, I know you are not an expert on local area networks. I believe the unclassified network has two basic threats. The first threat is viruses that can cause denial of service."

Bill: "Ringer, viruses are not a threat, that is all media hype. I can not remember a single virus that has infected our stand alone computers."

Ringer: "Bill, viruses can do damage. The LAN has to have an anti-virus program for detection of viruses. This program will be on the network so users can test for viruses. Additionally, the access to computer bulletin boards should be restricted."

Bill: "What, I think you are going too far. If I am not busy at work, I want to use the bulletin boards. Bulletin boards have excellent anti-virus software that we can use for free. The bulletin boards have graphic programs that can be installed on the network. Also, the computer bulletin boards are local calls."

Ringer: "First, bulletin boards should not be used for playing at work. Second, some bulletin boards are toll calls."

Bill: "I don't agree with you. What is the second threat?"

Ringer: "I believe the second threat is the user."

Bill: "The user. How can the user be a threat?"

Ringer: "I read an article that stated that more data is lost by non-malicious destruction of data by the user than through planned intrusion."

Bill: "Ringer, I disagree. The user is your greatest asset."

Ringer: "True, but the user can also be the greatest liability. People are not going to admit that they made a mistake. A backup system should be established to recover lost data. Also, training of the user is an important issue. The user can be the greatest asset if he/she is properly educated."

Bill: "Well, you may be right about the user. What type of electrical protection will the system have?"

Ringer: "I believe surge protection should be adequate."

Bill: "Ringer, you sound like an expert on these security measures. I vote for you as the LAN manager."

Ringer: "Bill, this is a small network of eight computers. A LAN manager is not required."

Bill: "Ringer, thanks for your time. I just want to repeat that controls are unnecessary in an unclassified environment. I believe the more controls imposed on the user the less productive the users will be."

Ringer: "Bill, thanks for your advice. I will do some more research on the subject."

The following week Token received the responses from all the department heads. Most of the department heads agreed on some restriction on access to the network. All the departments wanted access to the network from their house.

The department heads had three concerns about threats to the system. The major threat was denial of service if the system went down. The integrity of the data was the second threat. Finally, the confidentiality of sensitive data was the third threat.

Since the Department Heads had various ideas, "Ringer" decided to have a discussion meeting on LAN security. He invited the Operations Officer, Training Officer and the Maintenance Officer.

Operations Officer: "Ringer, I think we all agree that a backup system is required for a LAN. Of course, backups are essential for natural disasters."

Training Officer: "I agree. Also, we should have audit trails to detect and determine problems."

Ringer: OK guys. Who has the time to read all the information from the audit reports."

Training Officer: "I believe the Administrative Officer has plenty of time."

Ringer: "Thanks, but let's get back to the issues."

Operations Officer: "I believe the LAN should be centrally located. A cipher lock on the door will eliminate many of our physical security problems. The central location will make environmental protection items such as no eating or smoking easier to enforce."

CDR Corona: "I disagree. A centrally located LAN is not convenient or practical. The hangar is three football fields long. I will have no one to answer the phones. The LAN should be in the work spaces."

Ringer: "Well, I guess the CO will make the ultimate decision on the location of the LAN. Is the network cabling an issue? I read fiber optics is superior protection against tapping into the network."

CDR Corona: "Ringer, fiber optics may be out of our price range. I don't believe a threat is an intruder tapping into cable. The intruder probably could learn more about our operation from the local newspaper."

Ringer: "Well, if tapping into our cable is not a major consideration for cabling, what is?"

CDR Corona: "I am not an expert on cabling, but I would bet shielding against noise should be a consideration."

Training Officer: "I agree. Noise immunity may play a large factor in a noisy hangar environment. I bet an electric pencil sharpener can play havoc on a unshielded cable network."

Operations Officer: "I guess the big question is whether we should have unlimited access to the network. I

believe unlimited access in this unclassified environment is justified."

CDR Corona: "I disagree with unlimited access. We need some type of restrictions on files and directories. Everyone does not need access to all files. Fitness reports and enlisted evaluation can contain sensitive information. Additionally, users may get lazy and place classified information on the network."

Ringer: "I agree with the CDR Corona. Unlimited access is asking for security problems. Privacy Act information such as social security number, medical history and home address must be protected. Passwords may be required."

Training Officer: "Passwords are necessary. I think another solution may be to limit copying of diskettes by using diskless PCs."

CDR Corona: "First, we should connect the computers in the inventory and monitor the capability of the LAN. Second, I want to be able to use the computer when the network is down. I don't believe diskless PCs have that capability."

Ringer: "The last item to discuss is computer training."

Operations Officer: "Our personnel are adequately trained. I think a basic introduction into LAN operation and security should be adequate. Experience is the best training."

CDR Corona: "I want to emphasize that we are not dealing with sophisticated computer hackers in our organization. We are dealing with users who make honest mistakes. They should be adequately trained."

Operations Officer: "I think one area we should emphasize is user accountability. Everyone is accountable for their actions and this should be incorporated into security awareness training."

Ringer: "I would like to thank every one for coming today but our time is up. Thanks again."

After compiling all the data, "Ringer" decided it was time to eat. As "Ringer" was walking to lunch, he was stopped by

Lieutenant (LT) Bob Smith. LT Smith is the Communications Officer. "Ringer, when the LAN is installed I will order a Tempest check on the network. If the system passes Tempest, then we can place classified information on the network."

"Bob, this is an unclassified network. No classified information will be allowed."

"OK 'Ringer', I am just planning."

As "Ringer" started to write his proposal he had a dilemma. He already knew that the XO felt that the security issues were small items. He also knew that he would be working closely with the XO as the Administration Officer. He believed that definite areas needed addressing and decided to make the following recommendations:

- Recover system using backups required.
- Audit trails unnecessary.
- Anti-virus software on the network.
- Modem capability required. Therefore, remote logins authorized with a call back feature from the communication server.
- Train users on the fundamentals of the LAN.
- Minimal controls to increase productivity.
- Software purchased to blank screen when no key strokes in ten minutes.
- A risk assessment is not required since we had one three years ago and the assessment is good for five years.
- Limited access to the network with passwords required.

As "Ringer" was leaving the hangar, the clouds were returning for more rain. He wondered how secure a network should be and if he missed any of the problems. He knew time would tell.

D. TEACHING GUIDE

1. Overview

The case study is designed to examine security issues in a local area network (LAN). The case was developed so the students can discuss the problems and various control solutions. The student should be able to link the security problems with control measures after studying the case. This case assumes the student has basic security awareness.

2. Session Structure

The focus should be on security concerns when designing a LAN. What are the major security problems? How can they be resolved? Are hardware and software controls the only answer to a true secure system? Additional topics area discussed in the case were resistance to change, controls versus productivity, and perceptions that security is unimportant in a unclassified environment.

3. Class Discussion

The case was written in such a way that the officers in the case identified only partial solutions. The students can list the problems discussed and examine how each problem was handled. The following questions could also help direct the students to critical security issues.

- What are the security issues in this case?
- How validate are "Ringer's" recommendations?
- How important are the roles of the LAN's users in the successful implementation of a security program?

All the technical and managerial elements necessary to address security are developed in the remaining chapters of this thesis.

III. BASIC LAN TERMINOLOGY

A. INTRODUCTION

Before examining the security issues in a local area network, a brief discussion of LANs is presented for individuals not familiar with LANs. This chapter is a general overview of LAN characteristics. This is not a thorough description of LANs and can be skipped with no loss in continuity. For more technical information on local area networks the following books could be recommended: Local Area Networks: The Second Generation by Thomas W. Madron and Computer Networks, 2nd ed., by Andrew S. Tanenbaum.

The question is "What is a local area network?"

A local area network consists of a set of nodes which are interconnected by a set of links. The nodes may be terminals, microcomputers, minicomputers, mainframes, printers, hard disks or workstations. The links may be coaxial cable, twisted pair wires or fiber optic cable. [Ref. 3:p. 1]

In simple terms, a LAN connects computers together to share resources of information, hardware and has the ability to send messages within the network.

LANs usually have the following three characteristics [Ref. 4:p. 117]:

- A diameter of not more than a few kilometers. The LAN is usually networked in the same building or adjacent buildings.
- A total data rate of at least several million bits per second (MBPS).

- Ownership by a single organization.

Advantages of a LAN are [Ref 5:pp. 169-175]:

- LANs facilitate resource sharing of data, processing capabilities, data storage, communication lines, and output devices such as laser printers.
- Devices may be added to the network as the need arises. This is called modularity and provides for an orderly growth of services.
- LAN has electronic mail capability which allows messages to be sent from one linked computer to another.

B. LAN ARCHITECTURE

There are basically two logical architectures "that are supported on PC LANs today--peer-to-peer and client/server architectures." [Ref. 6:p. 51]

The peer-to-peer architecture "requires no dedicated file server because any node on the network may selectively share its local hard disk with other nodes on the network." [Ref. 6:p. 51] Since no additional hardware is required and the cost-per-node is usually lower, the peer-to-peer is a favorite choice of smaller organizations. The problem with peer-to-peer is a lack of a centralized database and lower performance. [Ref. 6:p. 51]

In the client/server architecture, services are provided by a file and a print server. The file and print server "do not provide any direct user application support, but provide an optimized design for file level I/O requests and spooled print services." [Ref. 6:p. 52]

The higher cost of a client/server architecture is "offset by higher performance and more sophisticated security provided by the software." [Ref. 6:p. 52] The advantages are the client/server provides better control of user access and backup operations than the peer-to-peer architecture.

There are three types of servers which are file servers, print servers and communication servers. The server "contains the hardware and at least part of the software, necessary to produce the service." [Ref. 7:p. 15]

Servers are usually located remote from the user and are "designed for multi-user access to expensive, complicated, or infrequently used services." [Ref. 7:p. 16]

A communication server "is a separate machine on the LAN that allows network users to connect to the outside world through one modem." [Ref. 8:p. 105] Communication servers are usually called either gateways or bridges. Gateways contain the "hardware and software necessary for two technologically different networks to communicate with one another." [Ref. 7:p. 18] For example, an ethernet and a token ring are connected via a gateway [Ref. 7:p. 18]. Ethernets and token ring terminology are discussed in Section D of this chapter.

Bridges are used to link two technologically similar networks. Combining two Ethernets would use a bridge. [Ref. 7:p. 18]

C. TOPOLOGY AND ACCESS PROCEDURES

Topology is the network configuration. The topology is described by Charles P. Pfleeger:

A single computing system in a network is often called a node, and its processor (computer) is called a host. A connection between two hosts is known as a link, and the pattern of links in a network is called the topology of the network. [Ref. 9:p. 368]

There are basically six types of network configurations. They are:

- Point-to-point.
- Multipoint.
- Star.
- Ring.
- Bus.
- Hierarchical.

A point-to-point is a simple network. It consists of a computer connected to one terminal. Multipoint is an extension of point-to-point in that instead of one remote terminal "there are multiple remote terminals." [Ref. 7:p. 11] A local network will normally have intelligence at all or most points on the system without the necessity for any central system. [Ref. 7:p. 13]

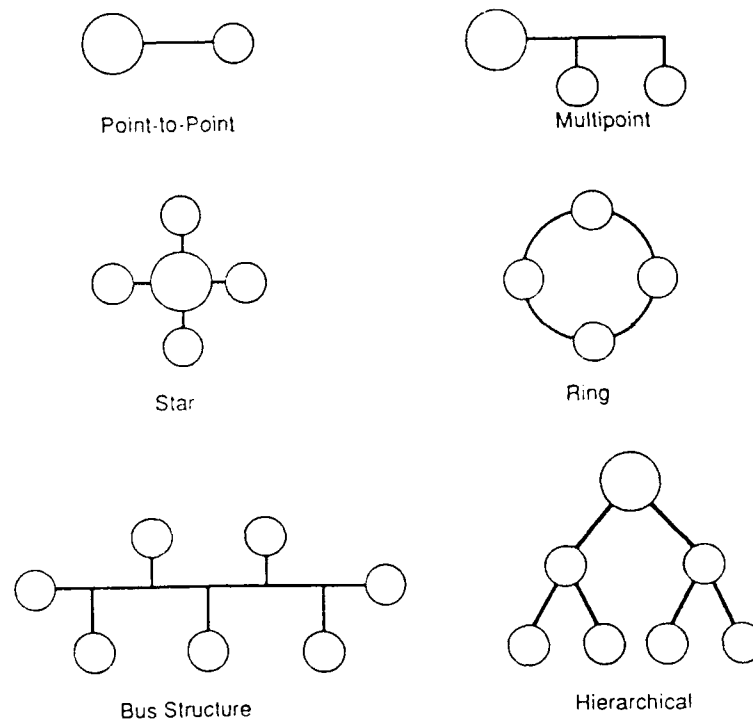
The star topology uses a centralized computer. All nodes communicate through the central computer.

The ring topology "is organized by connecting network nodes in a closed loop with each node linked to those adjacent on the right and left." [Ref. 7:p. 13]

The bus topology connects all the computers to one line or backbone. All the computers on the bus topology listen for a message for them.

The hierarchical network is a "fully distributed network in which computers feed into computers that in turn feed into computers." [Ref. 7:p. 13]

Figure 3.1 depicts the network topologies. The three most common topologies are the star, ring and bus.



Source: [Ref. 7:p. 15]

Figure 3.1 Network Topologies

The topologies "may be grouped according to the way in which signals are passed within them." [Ref. 5:p. 182] Broadcast and sequential are techniques for propagating signals that contain information. [Ref. 5:p. 182]

In broadcast, signals "are sent simultaneously to all nodes on the network." [Ref. 5:p. 182] Because each node has the possibility to communicate simultaneously, each node is in contention for the line.

The bus and star topologies support the broadcast mode. The main advantages are responsiveness and speed in a moderate size network. The disadvantages of the broadcast mode include extra expenses of detection and correction of collisions on the contention line and high installation expense. [Ref. 5:p. 182]

The sequential mode is used for point-to-point or ring topologies to pass data messages. Control is passed from one node to another to send or receive messages.

Network topology and access procedures are closely related. Access procedures are the rules for the nodes or microcomputers to communicate with each other on the network. These access procedures include [Ref. 5:p. 184]:

- Carrier-sense multiple-access with collision detection (CSMA/CD).
- Token ring.
- Token bus.

CSMA/CD is a collision-handling scheme that avoids the possibility of two nodes communicating at the same time on the network. CSMA/CD is used in broadcast topologies and has good performance at low to medium loads. The disadvantage is no guarantee of transmission for the node. [Ref. 5:p. 184]

The Token ring uses sequential control to give access to each node via a token. The token ring access method is "used within ring topologies that handle messages as discrete packets." [Ref. 5:p. 185] A token bus approach combines the broadcast characteristics of a bus topology with the control features of token-passing schemes. [Ref. 5:p. 185]

D. TRANSMISSION MEDIA

Local area networks use various media to provide services.

The transmission medium is the physical connection between network transmitters (sources) and receivers (destinations), bridging the distance between them. It may be a pair of wires, coaxial cable, radio waves, optical fibers, or infrared transmissions through the atmosphere. [Ref. 10:p. 35]

In designing a local area network, and for security purposes, the organization must consider the "characteristics of the medium, immunity to noise, and cost." [Ref. 10:p. 35]

The most common types of transmission medium are twisted pair copper cables, coaxial cables and fiber optics.

The oldest and most common transmission medium is twisted pair. "The twisted form is used to reduce electrical interference to similar pairs close by." [Ref. 4:p. 58] The

telephone system was the most common application of twisted pair.

A problem with twisted pair is that "copper wire has limitations for data transmission over distances of any magnitude." [Ref. 7:p. 27]

A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. The insulator is encased by a cylindrical conductor, often as a closely woven braided mesh. The outer conductor is covered in a protective plastic sheath. [Ref. 4:p. 58]

Coaxial cable is better than twisted pair in noisy environments. Coaxial cable is either baseband or broadband. Baseband coaxial is digital and uses a 50 ohm cable. The advantages include excellent noise immunity and high bandwidth.

Broadband coaxial cable is used in cable television and uses analog transmission. Broadband in computer networks means "any cable network using analog transmission." [Ref. 4:p. 60]

"One key difference between baseband and broadband is that broadband systems need analog amplifiers to strengthen the signal periodically." [Ref. 4:p. 60] "Baseband is simple and inexpensive to install, and requires inexpensive interfaces." [Ref. 4:p. 61] Baseband is adequate for data communication up to a distance of 1 km and is a single digital channel. Broadband is multiple channels and can transmit data, voice and video.

In fiber optics data are transmitted by pulses of light through non-conducting glass. "Currently available fiber optics systems can transmit data at or about 1000 Mbps for 1 km." [Ref. 4:p. 63]

Many of the problems inherent in twisted pair and coaxial are avoided with fiber optics, although the optic properties of cable can be affected by kinks or similar damage. The potential transmission speed of fiber optic cable is higher than coaxial, and coaxial is higher than twisted pair. [Ref. 7:p. 28]

Another advantage of fiber optics over coaxial is that fiber optics can run long distances without repeaters. "Security is excellent because fiber does not radiate and wiretappers will have as much trouble as the network owners in tapping it." [Ref. 4:p. 65]

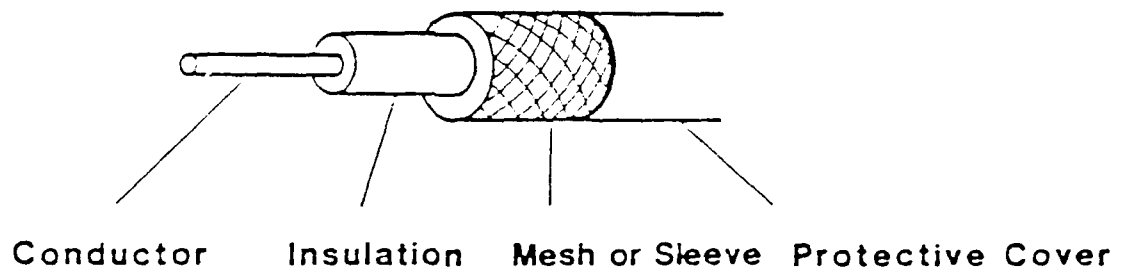
The disadvantage of fiber optics is its high cost. The optic cable may be superior for security purposes but may not be cost effective for information at the unclassified level. Figure 3.2 depicts the three types of transmission media.

Line-of-sight transmission is sending the data out into the air. "In particular, transmission by infrared, lasers, microwave, and radio does not require any physical medium." [Ref. 4:p. 65] Line-of-sight could be used between buildings when it may be expensive to dig the road up to lay a cable.

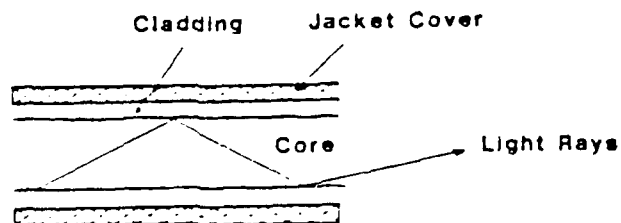
Laser or infrared communication is fully digital, and is highly directional, making it almost immune to tapping or jamming. On the other hand, rain and fog may interfere with the communication, depending on the wavelength." [Ref. 4:p. 65]



(a) Twisted pair.



(b) Coaxial cable strand.



(c) Optical fiber cable.

Source: [Ref. 11:p. 83]

Figure 3.2 Transmission Media

E. LAN STANDARDS OVERVIEW

The International Standards Organization's (ISO) Open Systems Interconnection (OSI) model "provides a general reference framework for LAN standards." [Ref. 7:p. 21] The model involves "connecting open systems--that is, systems that are open for communication with other systems." [Ref. 4:p. 14] The OSI model is separated into seven layers or functions. These seven layers are the physical, data link, network, transport, session, presentation and application.

The Institute for Electrical and Electronic Engineers (IEEE) 802 Committee "is attempting to provide standards that can be used to guide the manufacture of LAN components and software." [Ref. 7:p. 21]

The standards were written for CSMA/CD, token bus and token ring. "Standard 802.3 deals with Carrier Sense Multiple Access with Collision Detection (CSMA/CD)." [Ref. 7:p. 33] "A token passing bus standard is described by 802.4 standard and 802.5 defines a token ring system." [Ref. 7:p. 33]

F. COMPARISON OF LOCAL AREA NETWORKS

This section compares the strength and weaknesses of the three LAN standards.

CSMA/CD (802.3) is the most widely used today. A major advantage of CSMA/CD is that stations or nodes do not have to wait for a token to transmit. Therefore, delay of communicating at low level is basically zero. [Ref. 4:p. 163]

The major disadvantages of CSMA/CD are no priorities for transmission and drop in efficiency at high loads.

At high load, the presence of collisions becomes a major problem, and can seriously affect the throughput. 802.3 is not well suited to fiber optics due to difficulty of installing taps. [Ref. 4:p. 163]

Token Bus (802.4) uses "highly reliable cable television equipment." [Ref. 4:p. 163] "It is more deterministic than 802.3 and has excellent throughput and efficiency at high load." [Ref. 4:p. 164] Token Bus can support data, voice and video. Since a node must wait for the token to communicate, the token bus has a "substantial delay at low load." [Ref. 4:p. 164]

The token ring uses point-to-point connections and the throughput and efficiency at high load are excellent. "The use of wire centers make the token ring the only LAN that can detect and eliminate cable failure automatically." [Ref. 4:p. 164]

For people planning to run their LAN in overloaded mode, 802.3 is definitely not the way to go. For people planning to run with light to moderate load, all three perform well, so that factors other than performance are probably more important. [Ref. 4:p. 164]

G. SUMMARY

This chapter has provided a general review of the basics of local area networks and a general understanding of LAN terminology. The following chapter presents classifications of security problems in a local area network.

IV. CLASSIFICATION OF SECURITY PROBLEMS IN LANS

A. INTRODUCTION

This chapter addresses security in local area networks. Security issues are compiled from various sources into a security model. The literature on computer security is classified into five major areas: hardware security, data security, data communication security, physical security and human related security (Figure 4.1).

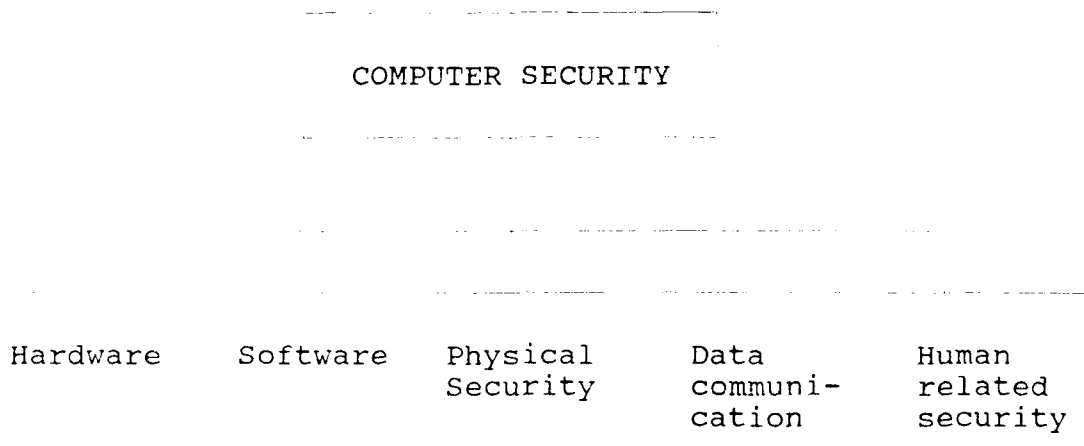


Figure 4.1 Components of Computer Security

In establishing a security program, the objectives must be clear and the threats identified. According to the National Computer Security Center, the three objectives of information security are [Ref. 12:p. 2]:

- Confidentiality of personal, proprietary, or otherwise sensitive data handled by the system.
- Integrity and accuracy of data and the processes that handle the data.
- Availability of systems and the data or services they support.

The threats to accomplishing these objectives include

[Ref. 12:p. 2]:

- Lack of awareness or concern for the implications of computer security issues.
- Carelessness, errors, or emissions.
- Equipment and media failure hazards.
- Intentional attacks by disgruntled or dishonest personnel, hackers, or hostile agents.

Different people perceive different threats. Aaron Brenner in the LAN Tutorial Series for LAN Magazine describes the three basic threats as [Ref. 13:p. 29]:

- Physical theft.
- Electronic tampering.
- Unauthorized access.

Physical theft involves employees "stealing computers, taking floppies with data, and tapping into the cable." [Ref. 13:p. 29] "Electronic tampering covers computer viruses and malicious reprogramming." [Ref. 13:p. 29] Unauthorized access involves employees seeing information they shouldn't see [Ref. 13:p. 29].

B. SECURITY

1. Hardware

a. Lack of Built-in Security Mechanisms

A personal computer has a lack of built-in security mechanisms. The typical personal computer does not support the following security mechanisms common to larger systems [Ref. 12:p. 4]:

- Multiple processor states--enabling separate "domains" for users and system processes.
- Privileged instructions--limiting access to certain functions (e.g., reading and writing to disk) to trusted system processes.
- Memory protection features--preventing unauthorized access to sensitive parts of the system.

Additionally, "few personal computers have hardware features that simplify installation of security measures such as a supervisor mode for sensitive instructions, hardware addressing limitations, or restricted access to input/output devices." [Ref. 12:p. 4] For these reasons "relatively unsophisticated attacks can overcome access control software or authentication techniques." [Ref. 12:p. 4]

b. Electromagnetic Emanations

Electronic equipment emit electromagnetic signals. Emanations produced by computers equipment "can be detected and translated into readable form by monitoring devices." [Ref. 12:p. 4] "Security measures intended to combat these

radio frequency emissions are known as 'Tempest' controls."
[Ref. 14:p. 84]

Tempest-certified hardware is secured from radio frequency (RF) emanations. The main concern of Tempest equipment is containment of its own RF signals. [Ref. 14:p. 84]

Although Tempest keeps the data from leaking or emitting, a relevant comment is made by Belden Merkus, an independent security consultant,

Tempest does not do all that it is supposed to do because there are some in the intelligence community who don't want it to be too good. Sidney Smith, an Anglican clergyman in England in the late 18th century said that the rat-catcher does not want to catch all the rats--otherwise he would be out of business. [Ref. 14:p. 84]

An emerging technology in the transmission of data in networks is RF LANs. RF LANs "allows very convenient computer networking without the burden of running cables to each terminal or computer." [Ref. 15:p. 225] Transmissions are sent via radio waves. This is a security eavesdropper's dream for information to be broadcast in the open. [Ref. 15:p. 225]

The U.S. Government has spent a fortune on containing accidental radio frequency emissions from equipment used in secure facilities through the TEMPEST program. It seems ironic that the very latest networking equipment should deliberately broadcast data over the airwaves. [Ref. 15:p. 225]

2. Software

a. License Violations

When an organization buys software it has an obligation not to sell copies, use for personal use, or use extra copies not specified by the license agreement. [Ref. 8:p. 105] Since license softwares are no longer copy protected, it is increasingly difficult for the organization to control unauthorized duplication of software.

b. Weaknesses of PC-based Operating Systems

The operating system performs the day-to-day computer functions automatically so the user is not involved in the basic operations of the system. MS-DOS is the most popular disk operating system for IBM-compatible personal computers. Because MS-DOS is so popular, numerous utilities are available "to do things like obviate copy protection, expose disk sub-structures and do sophisticated file/disk copying." [Ref. 6:p. 51] These utilities "expose all data on the local workstation or LAN file server to security risks." [Ref. 6:p. 51]

c. Viruses

Attention has focused recently on security of computers. National television and the press have stirred excitement about viruses in computer systems. Viruses are a small portion of the computer security problem. Peter Coffee in PC Week summarized by stating:

The virus problem is distracting valuable attention from threats that are far more common. Cheap, simple protection against those common problems will make you immune to most of the damage a virus can do. [Ref. 16:p. 46]

First, what is a virus when dealing with computers?

A virus is a program that can infect other programs by modifying them. The term virus arises because the infected program can be modified to include a copy of the virus program itself, so that the infected program then begins to act as a virus, infecting other programs. The viruses eventually overtake the entire computer system. [Ref. 9:p. 178]

A brief history of viruses is important to realize the threats of a virus. The cases discussed give insight on how viruses enter the system and possible consequences. It is important to realize that even viruses or games that were played in fun can disrupt work and overload the system. A virus can do damage such as crashing the system, erasure of data, or destruction of systems programs [Ref. 17:p. 21].

Some famous viruses include the IBM "Christmas virus," the Lehigh virus, the Jerusalem virus and the Internet worm. Each of these viruses are unique and will be discussed in general terms in the following paragraphs.

The IBM "Christmas virus" sent a Christmas greeting on the electronic mail system on the internal IBM computer network. When an individual attempted to clear the screen the virus went into the computer's distribution list and sent the message to everyone on the list. The Christmas

greeting spread exponentially through the network and eventually the network crashed. [Ref. 17:p. 21]

The Lehigh virus is so-named because it was discovered at Lehigh University in Bethlehem, Pennsylvania. The Lehigh virus is considered an active virus. "The active virus is a virus that damages or destroys systems." [Ref. 18:p. 26]

The virus hid in the Disk Operating System (DOS) in the COMMAND.COM file. This file is executed every time entries are made into the keyboard. Since the virus hid in the stack space of the COMMAND.COM file, the file size did not change. The changing of file size is usually a way to detect a virus but not in this case. [Ref. 18:p. 26]

Once the virus was in place, whenever a user typed a DOS command, the virus would check to see if there was a non-infected COMMAND.COM file on the system. If so, it infected it and incremented a counter that kept track of how many other disks it had infected. The virus would then execute the user's DOS command. All this, unbeknownst to the user. [Ref. 18:p. 26]

When the counter hit four, the virus would erase the hard disk, including the boot sector and the file allocation table (FAT). The virus did leave two trails. First, the date on the COMMAND.COM file would change. Second, the write light would be on the disk being infected. [Ref. 18:p. 26]

The Jerusalem virus was hidden in the install program on the master disk [Ref. 19:p. 26]. The virus made the news because it was supposed to strike on Friday, the 13th

of October. The virus did not cause major damage but emphasized that the network infected had no preventions against viruses.

The Internet worm downed over 60,000 PCs on the Internet. The Internet is a worldwide network connecting academic, business, and military computers. A worm is a type of virus which reproduces itself. [Ref. 20:p. 74]

As the above viruses illustrated, viruses are usually created for a specific software or hardware environment [Ref. 21:p. 25]. "MS-DOS based viruses may tag onto application programs such as .COM or .EXE files." [Ref. 21:p.26] This type of virus on DOS usually changes the file size and date [Ref. 21:p. 26].

Computer viruses enter the system in two ways. The user "enters an infected program into the system or telecommunication link allows a virus to cross from one system to another." [Ref. 17:p. 22] The second way is via telecommunications. "When telecommunications is the medium, dial-in access is often found, because dial-in opens the system to a sometimes hostile world." [Ref. 17:p. 22]

Even innocent activities can lead to a virus. An employee may bring a program to work from a computer bulletin board. Although the program is for personal use, the program is infected and the virus attaches to the operating system. [Ref. 17:p. 22]

In summary, there are certain aspects of networks that make networking a "virtual petri disk for breeding computer infection." [Ref. 20:p. 73] Michael Reimer, executive vice president of Cleveland-based Fountain Ware, says "the one-to-one relationship between PCs and users is one of the single greatest points of risk on the network." [Ref. 20:p. 73] Other points of entry for viruses include bulletin boards and diskettes. The threats to the system are the integrity of the database and service denial.

3. Communication

Remote connections are an easy and convenient manner to connect to a network from home or another network. A local area network with a modem capability can connect to another network. Remote logins are convenient to take work home and access the network from the user's personal computer. The problem is that "anything extremely useful and convenient that deals with sensitive data is a security disaster." [Ref. 22:p. 38]

The two major security problems with remote connections are illegal entrance by computer hackers and access to Bulletin Board Systems (BBS).

Since access is easy for users, access is also easy for the computer hacker. A problem with remote logins is that hackers attempt random numbers on the telephone until they obtain a dial tone and then enter the network or PC [Ref. 8:p. 105].

Second, if access to a dial-out modem is easy, uncontrolled download of files from the Bulletin Board Systems (BBS) may occur. Bulletin boards are a primary source of virus infection and many systems are toll calls [Ref. 8:p. 105]. Therefore, if dial-out lines are available, abuses may occur without adequate controls [Ref. 22:p. 38].

4. Physical Security

An important consideration in the design of a LAN is physical security. Physical security encompasses many areas and has lasting effects on the operation of the network. Physical security deals with locks, equipment and electrical power to mention a few. The most comprehensive definition of physical security is given by the Federal Property Management Regulations.

Federal Property Management Regulations define physical security as,

...the sum of construction features and the use of locks, guards, badges, and similar measures to control access to a facility (location) as well as the measures required to protect personnel and property, including the structures housing the computer, their contents, and related equipment, from, but not limited to, damage from accident, fire, loss of utilities, environmental hazards, and unauthorized access. [Ref. 23:p. 41]

Physical security in this section is divided into workstations, servers, diskette dilemma, cabling and environmental damage.

a. Workstations

With the growth of computers at home, the chances of stealing increases in the work environment. A defective board from the home computer can be easily swapped at work for a working board. Since the microcomputer is easy to access, computer parts can be swapped or stolen undetected. [Ref. 24:p. 15]

"The highest security risk in a LAN is the workstation." [Ref. 6:p. 52] The user has free access to DOS-based workstations which is convenient for stealing of sensitive data [Ref. 6:p. 52].

b. Servers

As discussed in Chapter III, the file server is the heart of the LAN. Most servers are unprotected against disk removal. Additionally, servers are subject to theft because of physical size. Uncontrolled access to servers could cause potential loss of data through misuse of the server console [Ref. 6:p. 52].

Another concern with servers is using personal computer clones.

Some LAN vendors repackage IBM Personal Computer AT clones and call them servers. This can be a source of problems, because a network server will be driven far harder than any AT. It is best to look for a vendor who builds minicomputer-like systems designed to work 24 hours a day for years. [Ref. 25:p. 19]

c. Diskette Dilemma

The diskette is the most common medium for the input and output of information from the computer. The advantage is that the diskettes are compact and easy to carry. The disadvantages are that they can easily be copied, stolen or damaged. [Ref. 24:p. 13]

The problem is that organizations place very little control on diskettes. Labelled and unlabelled diskettes are usually scattered around the working area of the microcomputer. End-users do not place a priority on security of diskettes. [Ref. 24:p. 13]

"Once the information is stored on the local disk, there are typically no security processes in place to prevent an unauthorized user from obtaining it." [Ref. 6:p. 51]

d. Cabling

Cable topology "is the basis for physical security." [Ref. 25:p. 19] The two major standards for cable topology are IEEE 802.3 (Ethernet) and IEEE 802.5 (token ring). The selection of token ring or Ethernet will affect reliability of the system. Token ring design has fewer active components. [Ref. 25:p. 19] Therefore, it is "easier to locate and isolate problems on a token ring." [Ref. 25:p. 19]

The tradeoff is that Ethernet failures occur less often than token ring [Ref. 25:p. 19]

Cabling is a major component of network stability and, because of the capital investment involved, one that is difficult to alter if improperly designed. Shortcuts

degrade security in ways that are difficult to quantify and correct. [Ref. 25:p. 19]

Cabling is not the area in which "low initial cost should be a design objective because of operational and security reasons." [Ref. 25:p. 19]

"Cable is one of the first and easiest places for a LAN security breach to occur." [Ref. 14:p. 84] Copper-based systems can be tapped easily. Twisted-pair or other copper cable don't need contact with the cable to be tapped. Instead, an electromagnetic pick-up and an antenna device can be built for under \$20. [Ref. 14:p. 84]

Another weak spot for LAN security is electromagnetic signal leakage or emanations. The cabling and the connectors, amplifiers and tap boxes leak a portion of the signal. "These leaked signals can be turned into readable data." [Ref. 14:p. 84]

A not-so-obvious security problem is running unshielded twisted-pair near electrical devices such as electric pencil sharpeners [Ref. 26:p. 96] "Electromagnetic radiation emanating from electromechanical and electronic devices can crash your system." [Ref. 26:p. 96]

"Fiber is somewhat more secure, since the loss of light caused by a tap is often detectable." [Ref. 14:p. 84] Fiber optics is not free from tapping. Since a connection is required to expand the network, the connections are the possible weak point [Ref. 14:p. 84].

e. Environment Damage

An important area in physical security is electrical power and effects on the computer system. The "quality and reliability of the network's electrical power supply" must be considered for the LAN to function properly [Ref. 27:p. 120].

A study completed by IBM and Bell Labs determined "that power disturbances occur on the average of two times a week for most commercial sites." [Ref. 27:p. 120] Additionally, the studies determined "that a large proportion of disturbances are generated within the building." [Ref. 27:p. 120]

A personal computer operates on 120 volt service. The American National Standards Institute (ANSI) define steady-state voltages for 120 volt service "as a continuous operation at a range from 108 to 125 volts alternating current (VAC) for 120 VAC." [Ref. 27:p. 120] So, a personal computer does not receive exactly 120 volts.

In the above mentioned study, the following power line disturbances were identified:

- Sags.
- Surges.
- Failures.
- Oscillations.
- Spikes or impulses.

"Sags are cycle-to-cycle decreases in the power line voltage below 80 percent of the nominal value lasting less than several seconds." [Ref. 27:p. 120]

A sag can cause two problems to the computer system. If a sag occurs, "it causes the computer power supply to detect low voltage on its output, resulting in computer shutdown." [Ref. 27:p. 122] This could cause loss of data if user was writing a file to storage at the time of the sag. Power blackouts can cause similar problems to sags. [Ref. 27:p. 122].

The problem becomes more severe if the duration of the sag "is approximately equal to the holdup time of the power supply in the computer." [Ref. 27:p. 122] This can "cause a reversal of the '1' and '0' in memory, causing the destruction of programs and data in RAM." [Ref. 27:p. 122]

"Surges are cycle-to-cycle increases in the power line voltage above 110 percent of the nominal value lasting less than several seconds." [Ref. 27:p. 120] Surges account for the majority of hardware damage and can stress computer components, especially power supplies [Ref. 27:p. 122].

Failures are a zero voltage or an outage. Failures can cause the same damages as sags.

"Oscillations or noise have a frequency range of 400 Hz to five KHZ, with beginning amplitude from 15 percent and up to 100 percent of nominal line voltage." [Ref. 27:p. 120] Oscillations rarely occur from wall receptacles.

Oscillations cause computer power supply and other hardware component damage. [Ref. 27:p. 122]

Spikes or impulses are an "over voltage superimposed on the line voltage waveform which lasts between 0.5 and 100 microseconds and has an amplitude over 100 percent of peak line voltage." [Ref. 27:p. 120] Spikes "are rapid excursions of voltage." [Ref. 27:p. 122] Spike/transient suppressors have become popular because spikes can cause destruction of computer hardware or damage software [Ref. 27:p. 123].

Table 4.1 summarizes the average frequency of disturbances in the United States, as determined by the IBM and Bell Labs studies. Power protection needs of a LAN usually rely on wall receptacle power "rather than a dedicated power line at the building entrance." [Ref. 27:p. 122]

5. Human-Related Security

The user is involved in many aspects of LAN security "If data resides on a LAN of fewer than 20 workstations with no connection to the outside world, how great is your exposure?" [Ref. 8:p. 100] The risk and exposure may be greater due to careless users than determined crackers [Ref. 8:p. 100].

The truth is "more data are lost and damaged through carelessness than through planned intrusion." [Ref. 8:p. 100] Mistakes made by an honest user may cause more problems than a computer hacker.

TABLE 4.1
FREQUENCY OF POWER DISTURBANCES

DISTURBANCE TYPE	OCCURRENCE PER MONTH	
	Building Entrance (IBM)	Wall Receptacle (Bell Labs)
Sag	1.5	4.0
Surge	1.0	0.3
Power Failure	0.6	1.0
Oscillation	26.0	not recorded
Spike	1.0	2.0
All Disturbances Per Week	7.5	1.8

Source: [Ref. 27:p. 120]

C. SUMMARY

Five areas were discussed and all play an integral part in implementing a security policy for LANs. As discussed in this chapter, the greatest security risk may be the user. Non-malicious destruction of data by the user is a definite concern. The following chapter examines the possible control solutions to the security problems discussed in this chapter.

V. CLASSIFICATION OF CONTROL SOLUTIONS FOR LANs

A. INTRODUCTION

This chapter surveys various control measures in local area networks. Although all the controls discussed may not be indispensable, it is important to be aware of the security and control issues when designing a local area network and planning for future expansion.

The amount of security will depend upon the threat perceived [Ref. 13:p. 29]. The most important area to consider for control measures is the level of security required for the network. The security level set will depend upon the importance of the data, the network utilized, and the availability of money [Ref. 13:p. 29]. "The level of security your installation requires is a big factor in what network operating system, security features and security equipment you should install." [Ref. 6:p. 54]

Classification of security needs could be categorized into three areas: low or no access control, medium access control, or high access control [Ref. 6:p. 56].

If no security controls are required, any network operating system (NOS) can function safely. Significant cost savings could be made in low access control by peer-to-peer architecture. [Ref. 6:p. 56]

Table 5.1 is the LAN security spectrum and provides examples of application types and suggested security features for a LAN.

TABLE 5.1
THE LAN SECURITY SPECTRUM

SECURITY REQUIREMENTS	APPLICATIONS	SECURITY FEATURES
Low/no access control	General office applications	<ul style="list-style-type: none"> - Peer-to-peer architecture - Password protection
Medium access control	Sensitive data, proprietary software	<ul style="list-style-type: none"> - Client-server architecture - Password protection - Access control to directories
High access control	Classified/secure data	<ul style="list-style-type: none"> - Client-server architecture - Password protection - Diskless workstations - Security monitoring - Access reporting

Source: [Ref. 6:p. 51]

A low security local area network can be characterized by the following [Ref. 6:p. 56]:

- Peer-to-peer architecture.
- DOS disk format.
- Bootable workstations (local storage).
- No required directory in file access control.
- Shareable printers across the network.

The spectrum of PC LAN security is very wide. Possible security features in a high access control are [Ref. 6:p. 56]:

- Dedicated file server.
- Non-MS-DOS disk format.
- Diskless workstations.
- Access control down to the lowest level possible file.
- Encryption of passwords.
- Security monitoring and accounting.
- Network encryption devices.
- Printers attached to secure file server.
- No remote login.
- Fault-tolerant design.

Most organizations are somewhere between the two extreme levels of the security spectrum.

Control issues for a LAN are divided into three major areas:

- Physical access.
- Logical access.
- Administrative controls.

Physical access deals with the controlling access to equipment. Logical access involves access to the data. This

type of access is the responsibility of the network operating system. [Ref. 6:p. 51] "It is via the NOS that 'logical' control for information access is carried out." [Ref. 6:p. 51]

Password access to servers, input/output (I/O) rights to directory or file structures, fault tolerance and user accounting features are all part of the support provided by a network operating system. [Ref. 6:p. 51]

Administrative controls involve upper management, the LAN manager and the user. All three are integral elements in designing a LAN.

Finally, the organization must assess the cost of the control measures versus the loss of software or hardware. "Security begins with an honest assessment of what you can afford to lose and how likely you are to lose it." [Ref. 8:p. 100]

A control's cost should be less than the resulting reduction in expected loss. This is dramatically indicated by the caveat--one should not kill a fly with a sledgehammer. That is, a control may be effective, but it will not be efficient. [Ref. 28:p. 14]

A good LAN security program involves prevention, detection and recovery. This is graphically depicted in Figure 5.1. This chapter examines these three areas.

B. PHYSICAL ACCESS

There are five methods of access control [Ref. 29:p. 202]. The first method is visual recognition of the individual by a guard or receptionist located at the point of entry. Visual recognition is used together with other methods of access

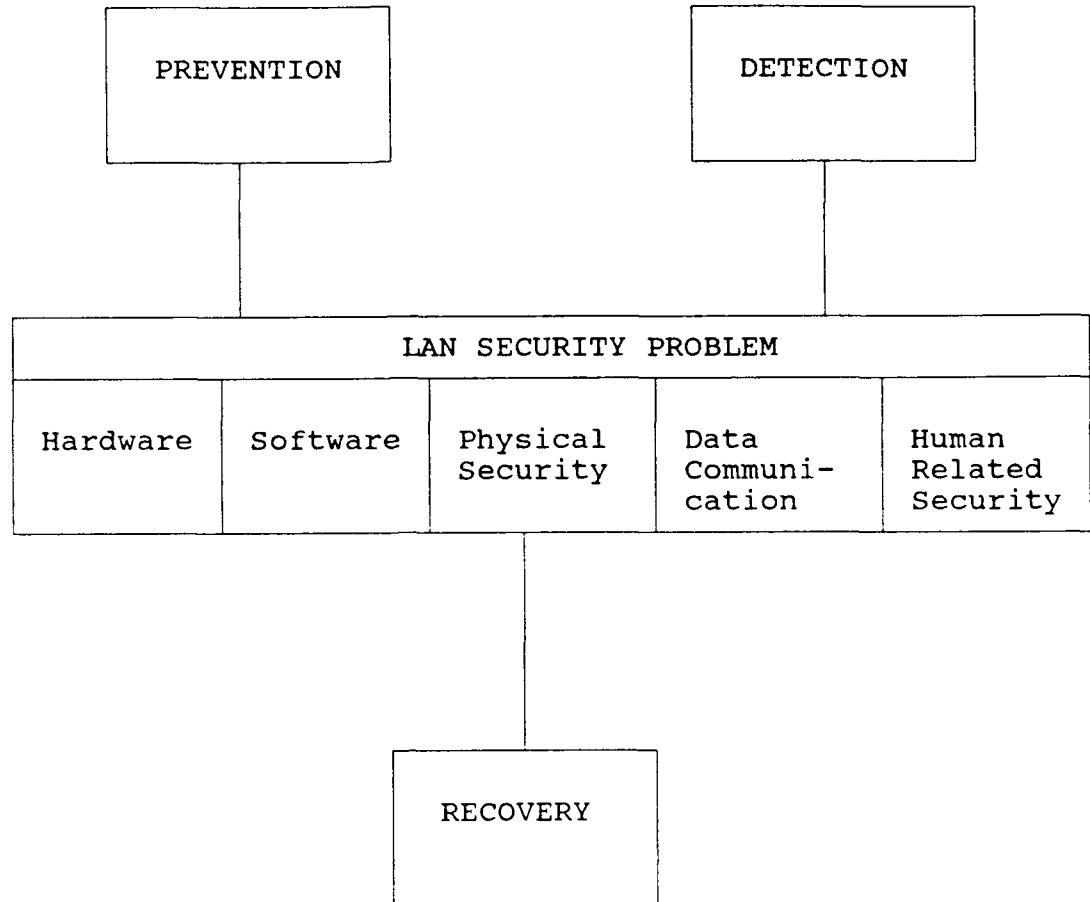


Figure 5.1 A Security Model

control. The second method uses a key to lock or a badge or card that activates some form of reader. Method three is based on combination to a lock or a password. A handwritten signature is the fourth method. The last method is based on measuring elements of the human anatomy. This method is called biometrics. [Ref. 29:p. 202]

1. Locks

Locks are the basic level to deter physical tampering of computer systems. The devices are inexpensive and range from \$20 to \$100. [Ref. 30:p. 108] Devices are available "that lock the PC's keyboard, on/off switch, backplate, or cover screw or one that locks your PC itself to the desk, floor, or any other permanent fixture." [Ref. 30:p. 108] "The most basic form of physical security is keeping equipment behind locked doors or bolting it to the floor." [Ref. 13:p. 29] This is a precaution for equipment being stolen.

Another method is to prevent physical access to the data on the computer. The lock on most PC ATs is an example of this measure. The PC AT lock is located in the front of the computer. When the system is locked the computer can not be booted and it is difficult to take off the computer cover. Most people are concerned with losing the key and not being able to use the computer so they do not lock the computer. [Ref. 30:p. 111] As in a lot of security issues, the lock has become more of a nuisance than a protector. A viable option is to keep the file server in a secure room or closet. This prevents direct access to the heart of the LAN.

Aarons and Raskin [Ref. 30:p. 108] state that board swapping is the next wave in nonmalicious tampering. Board swapping is malicious in an organization. "The best protection against board swapping, tampering, and messing

under the hoods are locks for the cover screw or backplate of the PC." [Ref. 30:p. 108]

In summary, locks are important to reduce theft but should be low profile. Otherwise, the PC may "look like a prisoner on a chain gang." [Ref. 30:p. 108]

2. Diskless PCs

Diskless PCs are another method of securing a LAN. Diskless PCs use no floppy or hard disk drive. The diskless PCs make it difficult to load viruses onto the network. And as important, "diskless PCs prevent users from stealing corporate information or software." [Ref. 31:p. 86]

Diskless PCs stop individuals from loading virus-infected software from bulletin boards and using unlicensed software.

The diskless PCs have two disadvantages. First, diskless PCs may have a hard time receiving acceptance due to previously purchased computers in the organization. Organizations desire to connect the computers already available rather than adding additional cost for more computers. Second, users need the capability to use the microcomputers when the network is down. [Ref. 32:p. 58]

3. Biometrics

Biometrics uses characteristics of an individual's body to gain access to a room or to a computer. The devices measure information that is unique to a person such as fingerprint, handprint, retina pattern, voice pattern or

signature. The body characteristics of the user are stored as models in the biometrics devices. Access is granted when the user's body characteristics are compared to the information stored in the biometrics device and confirmed. Access is denied if there is no match. [Ref. 33:p. 90]

The convenience of biometrics is their simplicity because there are no passwords, keys, badges to maintain or remember. For example, the retina pattern device obtains a scan of the blood vessel pattern in the retina. All individuals have a unique retina pattern and once these are verified, the user gains access. [Ref. 33:p. 90]

The major advantage of biometrics is the difficulty in duplicating an individual's body characteristics. At present, the major disadvantage of biometrics is the high cost. The second disadvantage is that errors do occur in the system.

Errors usually occur for two reasons. First, the quality of the measurement process is imprecise [Ref. 29:p. 202]. Second, "the human physical characteristics being measured by these systems can vary significantly from day-to-day and even within a particular day." [Ref. 29:p. 202] An illness by the user may cause a change in the metabolism to affect the readings of the biometrics device [Ref. 29:p. 202].

Errors experienced by biometrics access control systems usually are dealt with by permitting up to three attempts at securing entry before an individual is denied access by the device being used. When this occurs the individual involved usually is required to telephone a designated individual stationed within the controlled area and to secure admission through this person. [Ref. 29:p. 203]

A test was conducted to examine the reliability and ease of use of various biometrics. The devices tested included a retina verification device, a finger/thumb verification device, a hand-geometry identification device and a signature-verification device. The test results are shown in Table 5.2.

TABLE 5.2
RESULTS OF BIOMETRICS READINGS

Device	1st Attempt	2nd Attempt	3rd Attempt	Rejected
Eye	10			
Finger	20	5		
Thumb	12	10	2	1
Hand geometry	21	4		
Signature	9	1		

Biometrics are extremely accurate. The importance of the initial entry measurements can not be over-emphasized. Most devices at the end of the initial entry give a number for the quality of the data. This usually determines ease of access and how many attempts the user will have to try for access.

The eye and the signature survey were conducted using two separate days for testing with five attempts each day. The finger, thumb and hand-geometry test involved one week of

testing with five attempts completed each day. Each test allowed three attempts at entrance before the device denied access. The reason for a five-day test on these devices was to determine if the day-to-day metabolism could change access. It appeared that changes in metabolism had a small affect on the results. The major discrepancy with the thumb device was due to trying to determine the position for the thumb on the device. Since the finger and thumb use the same device, the thumb always overlapped the position holder. Unable to place the thumb in the exact same position each day resulted in a varying success rate.

The most secure system and easiest to use was the retina verification device. The user was verified the first time in a trial of ten attempts.

Signature verification equipment was the least secure for biometrics security equipment. The author gained access on signature on the first attempt every time. The problem was one student was able to duplicate the rhythm of the signature while copying the signature, and gain access. No other device accepted forgeries.

As the prices drop for biometric devices, this technology could be used in the start-up procedures for a local area network. [Ref. 22:p. 43]

4. Passwords

One of the forms of user authentication is passwords. Passwords are a simple and effective method to control access

to a computer and network. "A user must know a legitimate password to gain access to the system." [Ref. 14:p. 84] Because of the user's tendency to share passwords and keep the same password for years, passwords must be managed.

Selecting passwords correctly is fundamental to any security program. The object is to select a password of which other users and computer hackers can not make an educated guess and predict the password. The problem is users pick easy passwords such as first name, last name or display the password directly on the computer. [Ref. 14:p. 84]

Perhaps 10% of all computer accounts use between 50 and 60 common passwords. This reduces the effective number of passwords from 208 billion to 600--which are very good odds indeed. This is an area where hackers use custom computer programs. Their machine can call your system over the phone lines. [Ref. 34:p. 42]

The following list of do's and don't's are presented to assist in password development [Ref. 35:p. 6]:

- Don't use your login name in any form (password system may have a login name such as your name).
- Don't use your first or last name in any form.
- Don't use your spouse's or child's name.
- Don't use other information that is easily obtained, including license plate numbers, telephone numbers, social security numbers, the brand of your car, the name of the street you live on, etc.
- Don't use a password of all digits, or all the same letter that could significantly decrease the search time for a cracker.
- Don't use a word contained in dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.

- Do use a password with mixed-case alphabetic.
- Do use a password with non-alphabetic characters, e.g., digits or punctuation.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly. This makes it harder for someone to steal your password by watching over your shoulder.

There are many different strategies for selecting a password. These various strategies for picking passwords are summarized in Table 5.3. Table 5.3 provides example of different strategies and the security level of each strategy.

The first strategy is to have no password or type in the words "password or XXXX." The second strategy is to pick something easy to remember like "sex, drugs, etc." These passwords are easy to remember and popular but have a low security level. [Ref. 34:p. 42]

The third strategy is to have a random generator pick passwords using upper-case, lower-case, numbers and punctuation. An example of this would be "Z#Lu%p*v." This method would apparently be the best method. The problem is the password is so random that users can not memorize the code and must write the password down. Usually, this is done next to the computer. The protection against attack is poor and not a recommended strategy. [Ref. 34:p. 44]

The fourth method is to use "long, but misspelled, common English words." [Ref. 34:p. 42] An example of this would be spelling computer as "computre." The security level

TABLE 5.3

PASSWORD STRATEGIES

	Strategy 1	Strategy 2	Strategy 3	Strategy 4	Strategy 5
Method	Pass- words? Weren't they install- ed by the manufac- turer?	Users select their own pass- words.	Assign random pass- words.	Long, but mis- spelled, common English words.	Pseudo- random pass phrases.
Security level	Nil. Can be, and is broken by unintel- ligent 11-year- olds.	Low. Regular- ly broken by intelli- gent 14- year- olds.	Low. Pass- words are so random that employ- ees can not re- member them.	High. These are not likely to be cracked by amateurs or dic- tionary sweep programs if unusual words are chosen.	Very high. Provides good combin- ation of upper and lower case letters as well as punctu- ation.
Examples	No password PASSWORD XXX	Sex Money drugs	6fTa.8Ac P[q4lMn lKaH%%u	Computre expandly rivrerun	IsjtAi53 WRa81?Ge TBlatStd
Protec- tion	None	None	Poor to none	Good	Very good
Conclu- sion	Not recom- mended	Not recom- mended	Not recom- mended	Recom- mended	Highly recom- mended

Source: [Ref. 34:p. 42]

in this strategy is high and the passwords are hard to duplicate. [Ref. 34:p. 42]

The last and fifth strategy is using pseudo-random, pseudo-phrase passwords. This strategy is "theoretically almost as secure as true random generation." [Ref. 34:p. 44] "The user invents an eight-word phrase and enters the first letters of each word." [Ref. 34:p. 44] Examples of this strategy are provided below [Ref. 34:p. 42]:

- IsjtAi53 = "I stupidly joined the Army in 53."
- WRa81?Ge = "Wong's Restaurant at 81st? Great eats."
- TBlatStd = "Twas Brill Lig and the Sly they doves" did gyre and gymbble...(thanks to Lewis Carroll).

The Department of Defense also emphasized certain areas for passwords. The recommendations from DoD Password Management Guideline include [Ref. 36:p. 2]:

- Users should be able to change their own passwords.
- Passwords should be machine-generated rather than user-created.
- Certain audit reports (e.g., date and time of last login) should be provided by the system directly to the user.

Finally, a password policy should be developed. First, passwords should not be written down or stored on a file on the computer. By writing the password down or storing in a file the user is dependent on the security of the file or paper. Second, users should not give passwords to others. By giving out the password, the user does not know if the

password will be distributed further. Third, passwords must be changed periodically, about twice a year. [Ref. 35:p. 6]

C. RECOVERY CONTROLS

1. Backups

Backup procedures involve making copies of the programs and the data files. Backups represent the ultimate protection against infections from viruses and employees who accidentally delete files and erase entire directories.

There are different types of files that should be considered in the backup system. These files include [Ref. 37:p. 105]:

- Hidden files containing the master lists of all network names and passwords.
- Security files, which list the rights and privileges of each network user.
- Files that have been stored by individual network users on their hard disks.

When backing up three types of files, a LAN backup "requires enough storage space for all of the data on the LAN's shared hard disk, and in some cases, individual users' hard disks as well." [Ref. 37:p. 97]

There are two types of backup options: backup to disk or backup to tape. Backup to floppy disk takes a considerable amount of time and an abundance of disk. The second method under-disk is to backup to another hard disk or to a removable hard disk. A removable hard disk enables the user to replace the broken hard disk easily. The only problem is that current

removable hard disks only have a capacity of 40 megabytes (MB). [Ref. 38:p. 23]

Backup to tape is the most popular method. The advantages of tape backup are convenience and less expense. The tape devices can be mounted internally in the 5-1/4 inch slots on the PC, but most are attached externally [Ref. 38:p. 23].

A new option is optical disk. This option is better used for storage of data than backup since the data on Write-Once-Read-Many can not be changed [Ref. 38:p. 23].

Backups should be completed as the situation demands and a grandfather system should be used. In extreme cases backups could be performed several times during the day, but at the minimum once a day. [Ref. 8:p. 107]

Grandfathering uses a system that insures important data is not lost because of various problems including viruses. First, backup every file in the LAN and this is the baseline. If the entire system fails, this is the backup to restore the system. [Ref. 8:p. 107]

Second, make daily backups, which you keep until the end of the week. At week's end, you do the weekly backup, which you keep for a month. Return the daily tapes to use for next week's backups.

Now, each month, do a monthly backup, which you keep for a year. Thus, you have four dailies. On Friday, you keep a weekly. At the end of the month, you have four weeklies. At the end of the year, you have 12 monthlies. And you always have the baseline backup. Only backup files that change (incremental backup). Then when you need to restore an entire drive, you start with the baseline and then update with the most recent incremental backup. If you find a virus in your backup, you can move to an earlier backup

(that's why you grandfather) and the worst you'll have to do is reenter a month's worth of data. [Ref. 8:p. 107]

The backup is usually not perceived as crucial until data are lost. With a local area network the system must be designed with a backup. An effective backup system is required because of the many users and amount of important information in the databases. [Ref. 37:p. 97] As will be discussed later in this chapter, more information is lost by nonmalicious employees than by viruses and stealing.

In summary, backup is only effective if done on a regular basis. "A good rule of thumb is backup the files that change every day, and backup the program executable once a week." [Ref. 38:p. 24]

2. Audit Trails

Once an individual penetrates the system, "security issues revolve around detecting breaches and identifying who is committing them." [Ref. 14:p. 88]

An audit trail is a program that constantly records information about what is going on the network--who is logging in and out, who is running what application who is deleting what file. It's often possible to detect and identify an intruder with an audit trail. [Ref. 14:p. 88]

Audit trails have two drawbacks. An obvious problem is that someone must have the time to read all the recorded information and understand it. "In a LAN, people record their hearts out but nobody ever looks at it," says Peter Krauss of LAN VAR LAN Services (New York, NY). The LAN manager should

review audit trail at least once a week for anomalies. [Ref. 14:p. 88]

Another problem is that audit trails use a large amount of disk space. This disk space problem can be reduced by monitoring the network at certain hours. Of course, restricting audit trail hours reduces security. [Ref. 31:p. 88].

Since every transaction is recorded on the network, an audit trail is an effective security tool. [Ref. 31:p. 88]

3. Disaster Recovery Plans

Disaster recovery is for a major catastrophe such as a fire, flood, earthquake or disk crash. The organization must determine how extensive the recovery system should be. As mentioned in the backup section, "recovery schemes depend upon the importance of data, the quantity of data, your budget and the time the system can be down." [Ref. 39:p. 32]

A disaster recovery plan may involve fault-tolerant features. Fault tolerance is "protection of data against hardware failure." [Ref. 6:p. 54] Fault-tolerant features "include redundant servers, hardware, disks, utilities and files." [Ref. 39:p. 32]

Two methods of fault tolerance include disk bad-track handling and mirrored disks. Disk bad-track handling recognizes that "every disk has flaws and important for software to deal with this transparently." [Ref. 6:p. 54]

Mirrored disks is "writing data to two separate disk drives so both drives will contain the same logical data." [Ref. 6:p. 54]

Before considering expensive fault-tolerance features, one should consider the basics. The basic steps before fault-tolerance systems are power protection and tape backup. Since the servers are constantly on, the servers should be protected by an uninterruptable power supply (UPS). [Ref. 40:p. 60] "A UPS is basically a huge battery." [Ref. 40:p. 202] When the power is lost, the UPS starts to work.

Additionally, fault tolerance does not take the place of tape backup. For example, if a virus infects one disk, the other disk is automatically infected with disk mirroring. [Ref. 40:p. 60]

D. DATA SECURITY CONTROL

1. Virus Prevention and Detection

Prevention is the most important area when dealing with viruses. Knowledge of proper procedures and anti-virus programs can save the organization many headaches.

The first preventive method is to "limit network access to legitimate users." [Ref. 41:p. 78] This involves proper password security procedures and an operating system that grants access to data on a need-to-use basis [Ref. 41:p. 78].

Secondly, anti-virus software is on the market to deal with viruses. "Common elements of anti-virus software are programs that monitor, detect and protect against virus infection." [Ref. 21:p. 28]

Pirated programs and free software should not be used. These programs could carry a virus. Ensure the anti-virus programs purchased are not viruses in disguise themselves. To prevent this, "centralize software purchasing or have an approved vendor list." [Ref. 18:p. 27]

The computer bulletin board systems (BBS) are susceptible to viruses. Restrict the use of dial-out lines and restrict access to the BBS. Software is available to restrict the access to only approved telephone numbers. Since viruses run from executable files, files ending in .EXE or .COM, users should not copy executable programs from the bulletin boards. [Ref. 8:p. 105]

Besides anti-virus programs and using original software, the most important element is to test the software on a separate personal computer before installing on the network. By testing on an isolated computer this precludes the virus from infecting the entire network. [Ref. 41:p. 78]

Preventive measures for viruses are listed in Table 5.4.

If the prevention methods fail, how are the viruses detected? If the virus is complex, the virus may not be

TABLE 5.4
PREVENTIVE MEASURES FOR VIRUSES

-
1. Limit network access to legitimate users.
 2. Centralize software purchasing or have an "approved" vendor list.
 3. Don't use unknown software.
 4. Use a write tab on "suspect" disk.
 5. Instruct employees on the dangers of viruses.
 6. Make all .EXE and .COM files on PCs read only.
 7. Test all new software on an isolated system before loading on network.
 8. Make working copies of all original diskettes.
 9. Check system programs, utilities, and applications regularly for unusual behavior.
 10. Remove any suspicious programs with a utility that completely overwrites the disk space formerly occupied by the deleted files.
 11. Make frequent backup copies of files.
 12. Log all access or attempted accesses to the network.
 13. Never boot a hard disk system with a floppy disk.
 14. Use Anti-virus programs.
 15. Restrict access to bulletin board systems.

Sources: [Refs. 41:p. 78; 18:p. 27]

detected until it is too late. A few methods for detecting virus are [Ref. 18:pp. 28-29]:

- Check file sizes against a previously established table.
- Use utilities or programs that search all program files for strange text.
- Set system clock to the future.
- Look for strange files on the system.

Once a victim of a virus, the computer should be pulled off the network and the virus isolated. If the virus is detected early, then the backup tapes can be used for restart. Before reloading, turn off the power to the system to ensure that random access memory (RAM) is cleared. If the virus is complicated, a computer expert should be called. [Ref. 18:p. 29]

Backups are the primary method of recovering from a virus. Copies of original vendor software should be made as a backup.

If viruses cannot be prevented or cured, it is essential that the means be available to recover from them. Only thorough backup can make that possible. [Ref. 17:p. 23]

Finally, anti-virus programs alone are inadequate to provide the necessary prevention against viruses. To preclude future viruses a strong prevention program including anti-virus programs and backups are recommended. The bottom line is viruses require effective controls of software and responsible personnel. "Effective, security-conscious,

vigilant management is the solution to computer viruses, as it is all computer security problems." [Ref. 17:p. 23]

2. Operating System

Once access has been gained into the network, controls should be set for the type of data the user can access. Currently, most network operating systems have file security systems. [Ref. 14:p. 85] The file security system enables the LAN manager to "determine directories and even individual files a given user can have access to." [Ref. 14:p. 85] The LAN manager can also "set the type of access, determining whether the user can only read a file or whether he has full read/write access." [Ref. 14:p. 85]

In this way, there can be a whole hierarchy of security within a system, allowing certain users access to directories A, B, C and the accounting database, while others have access to directories D, E and F and the inventory database. Access must also be controlled to programs. There must be a way to prevent users from running programs they do not--or should not--need. [Ref. 14:pp. 85-87]

3. Encryption

If the data are valuable or classified, then the lines should be secure. One way of doing this is encryption. Encryption codes the information before the data are sent on the network. Encryption "is one of the best security methods for local links." [Ref. 22:p. 38] "For remote connections, encryption is the only answer to keep information secure." [Ref. 22:p. 38]

Encryption is not widespread because it costs money. "An encryption program costs twice the price of a LAN card." [Ref. 14:p. 88] An unclassified or low security-level system would not require encryption of data. Presently, encryption slows the network by the time required to code and decode messages. Many LAN managers just encrypt passwords because encryption is expensive. [Ref. 14:p. 88]

E. COMMUNICATION

When a legitimate need for dial out is required, use a communication server. As discussed in Chapter III, the communication server allows the users to connect to other networks through one modem. A combination facsimile and modem board provides "the advantage of making both dial out and fax available to all network users." [Ref. 8:p. 105]

All users rarely need outside connections. When they do, however, use the communications server approach and write scripts that automate (and restrict) the outside numbers to which users can connect. [Ref. 8:p. 105]

Three basic rules apply when using remote access in LANs [Ref. 22:p. 38]:

- Should have dial back where the system (modem) dials the authorized user back after calling.
- Turn the modem off when not in use.
- Limit the number of tries with the wrong password.

The most important rule for remote access is "no outside access when dealing with sensitive data." [Ref. 22:p. 44]

F. CABLING AND ELECTRICAL DESIGN

1. Cabling

The type of cabling is an important security decision. Fiber optic cable is "far more resistant to wiretapping than other media and should be considered for applications where security is important." [Ref. 15:p. 227]

The biggest benefit from fiber optics in terms of data security, may be noise immunity. Since fiber optic cable uses light as a transmission source, it neither emanates nor is it susceptible to emanations from other sources. Fiber optic cables may be run next to electric motors without experiencing any interference from the motor's field. As long as the cable is physically, it is virtually impossible to tap. [Ref. 42:p. 140]

Additionally, fiber optic physical security is "less expensive than for traditional wire cables since fiber optics require no electrical shielding." [Ref. 8:p. 140]

Connections is another concern with cabling.

By placing all connections in a locked wire closet and providing diagnostic taps and tools, the system is protected against vandalism, troubleshooting is faster and the network can be restored to service more rapidly in the event of a cable, tap or access unit problem. [Ref. 25:p. 19]

Laying the cable is an important area in designing a network. Although laying the cable the shortest distance is ideal, it may be more headaches than it is worth. Ideally, the LAN manager needs to access the cable for troubleshooting if required. For this reason proper documentation of cabling layout is required. [Ref. 39:p. 33]

The cable tips are summarized below [Ref. 43:pp. 124-125]:

- Double up each line. Run two cables instead of one.
- Use wall plates. Looks better also keeps tension off the drop cable.
- Avoid running copper cabling near power wires and florescent fixtures. Watch out for electromagnetic energy. An electric pencil sharpener can wreck havoc on a network.
- Think about future requirements.
- Check the codes and regulations before installing cable
 - * Local fire codes.
 - * National Fire Protection Association Standards.
 - * The National Electrical Code (NEC).
 - * Local and national building codes.
 - * Uniform Building Code.
 - * FCC regulations against Radio Frequency Interference (RFI) and Electromagnetic Interference (EMI).
- Avoid placing cable in areas where it can be damaged.

Realistically, tapping an unclassified network would be considered a low probability and risk. As discussed, the shielding of the cable is an important element for noise immunity. In designing a low-risk LAN, the noise factor should be more of a consideration than tapping threats.

2. Electrical Power

Electrical power is an important security area for LANs. Electrical protection should cover the file server and other critical systems.

An IBM study determined "that uninterruptable power systems (UPS) are required for the reliable, continuous

operation of electrical equipment." [Ref. 27:p. 123] On-line UPS may not be cost-effective for all computer applications. At the minimum, surge power protectors and back up power are required.

As depicted in Table 4.1, there are 1.8 power disturbances per week from wall receptacles. Since PC-based power is from wall receptacles, this is a vulnerability for equipment operating continuously as a file server. An on-line UPS is a cost-effective solution when the equipment is running on a continuous basis such as the file server [Ref. 27:p. 124].

G. MANAGEMENT CONTROLS

A neglected aspect of LAN security is the LAN manager [Ref. 6:p. 52]. The LAN manager is "responsible for setting up passwords, access rights, recovery and backup procedures, and monitoring the system for security violations." [Ref. 6:p. 52]

"It doesn't matter whether you have a two-node LAN or a 200-node LAN, the LAN needs a LAN administrator." [Ref. 26:p. 96] Although managing an entry-level LAN is only a collateral job, someone must be responsible for monitoring the system.

It is important to "train more than one person as the LAN manager." [Ref. 39:p. 33] Otherwise, if the LAN goes down when the LAN manager is gone, all the work stops. "A LAN manager must understand DOS and the networking operating

system, know how to do backups and to troubleshoot problems."

[Ref. 39:p. 33]

Management should evaluate their microcomputer environment to ensure that the proper controls exist. Management should

[Ref. 44:p. 27]:

- Develop and disseminate data security policies and procedures to all employees.
- Analyze information in terms of its confidentiality and sensitivity.
- Implement appropriate security measures over information deemed confidential or sensitive.

Management must "balance ease of use with security controls." [Ref. 45:p. 28] "Security measures must be designed in a way which will encourage user compliance."

[Ref. 45:p. 78] Access control measures such as "log on security, passwords, physical access controls--terminal lock and key, card-reading devices or biometrics--and terminal identification are of no help if they are ignored or circumvented." [Ref. 45:p. 78] The organization must "strike a balance between absolute impregnability and user convenience." [Ref. 45:p. 78]

Basic security objectives and security requirements should be "identified at the beginning to avoid needless replication and to conserve resources." [Ref. 46:p. 24]

"Security is as much about preventing data loss from errors as it is about preventing intrusion." [Ref. 8:p. 108]

"Security is meant to keep your business your business. But

it's also meant to help users do their jobs safely and conveniently." [Ref. 8:p. 108]

Security is an attitude. Security must be emphasized from top management down. Time allowance for training and security awareness is essential. A large portion of damage to computers is unintentional and non-malicious from untrained personnel. Security awareness for new personnel is required when introducing proper procedures for using microcomputers and networks. "Training is expensive, but not nearly expensive as not training." [Ref. 47:p. 24] The most effective security measure is the trained user.

Training is an important control ingredient. Initially, users should be grouped by skill levels: "whether they are new, familiar with DOS, familiar with word processing, or experienced users." [Ref. 39:p. 33] Then the application courses can be designed for different skill levels. Experienced users may only need training on areas unique to LAN operations. [Ref. 39:p. 33]

"Many control problems in the microcomputer environment are due to inadequate computer training." [Ref. 44:p. 26] Users without training "are not aware of pertinent backup, programming and security issues." [Ref. 44:p. 26] "Training employees on the proper uses of a computer system and the responsibilities associated with its use is the key variable in the development of a well-controlled environment." [Ref. 44:p. 26]

"Surprisingly, simpler controls are often better able to withstand the tests of time because they are understood by management and others who must support them." [Ref. 28:pp. 14-15]

The final decision on LAN configuration "becomes a matter of cost, support of required features, ease of installation and required administration overhead." [Ref. 6:p. 56]

The bottom line for security is very simple. Decide what you realistically need in security with your risk and exposure assessment and then apply the security measures. Have a disaster recovery plan and a written security document that lays down policies and procedures. [Ref. 8:p. 108]

Finally, "plan your network with an eye to the future." [Ref. 42:p. 141]

H. THE USER

Without the understanding and cooperation of the user of the system, the security policy and control solutions will be inadequate. The user will either suppress the controls or suppress the automated system [Ref. 48:p. ix]. When designing a LAN system, the effects of security on the user must be considered. "Security imposes restrictions which can cause friction." [Ref. 13:p. 30]

Personnel can become frustrated by security measures and attempt to circumvent the controls [Ref. 13:p. 30]. Users will not conform to restrictions if they don't understand the reasons.

A solution to this problem "is to motivate people to cooperate." [Ref. 13:p. 30] Mike Hurwicz suggests the following actions [Ref. 13:p. 30]:

- Explain the reasons for security procedures. When people understand why controls are necessary, they are more likely to cooperate.
- Make it clear to prospective and current employees that everyone is expected to cooperate. Establish clear consequences for failure to cooperate.
- Be specific about policies and procedures. Write them down and give everyone a copy.
- Don't overdo it.

Says Hurwicz, "Enlisting the support of employees is probably the single most cost-effective security precaution a company can take." [Ref. 13:p. 30]

End users have a security responsibility. Users must realize the "importance of keeping passwords to themselves and logging off their computers at lunch time and also at the end of the workday." [Ref. 45:p. 78] At the end of the day or when no one is working at the station, sensitive information should be cleared from the workstation including what is residing on accessible memory. Sensitive material must be properly protected and secured. [Ref. 23:p. 42]

Any security program must involve the user. The user must be indoctrinated in why these procedures are necessary. Additionally, the user must be security awareness trained.

Table 5.5 is a list of responsibilities that the user should have for a PC but can also be applied for local area networks.

TABLE 5.5
PC USERS' RESPONSIBILITIES

-
1. Properly securing sensitive information/data and media to protect against unauthorized destruction and access.
 2. Protecting PC equipment and media against the detrimental effects of dirt, heat, coffee, magnets, etc.
 3. Labeling PC-generated information/reports to differentiate them from normal data processing-produced data to include the creator's name, date, source, cop number, etc.
 4. Properly documenting programs to facilitate the turnover of files to new users.
 5. Complying with software licensing agreements.
 6. Making backup copies of essential files and programs.
 7. Preparing labels for PC media. (There should be a standard labeling format for the entire organization.)
 8. Prohibiting unauthorized access to information.

Source: [Ref. 23:p. 41]

Often the users comply with the hard regulations and rules, but the simple and common sense security measures are

often neglected. Common sense can go a long way to assist in the prevention of security problems.

The link between management controls and the user are training, trust and cooperation. Figure 5.2 depicts the User Security Asset Triangle. To have an effective user security program all three areas of the triangle must be developed. For example, training users leads to cooperation and develops a trust of management.

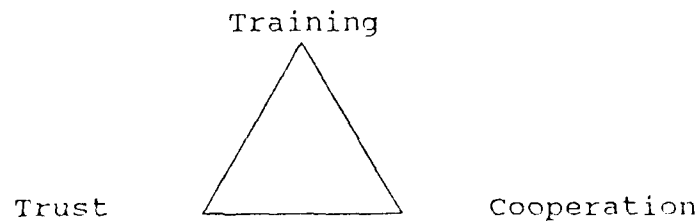


Figure 5.2 User Security Asset Triangle

In summary, the user is the most important asset and also the greatest liability [Ref. 18:p. 30]. The organization's security program is only as good as the user. Leaving passwords attached to the computer and the key in the computer are habits that should be avoided.

I. SUMMARY

This chapter has emphasized the prevention, detection and recovery elements as an integral part of system design. The fundamental elements of a LAN design include access protection, communication protection, management controls,

user interface and a recovery system. Each of these areas must be examined to ensure a good LAN design.

As discussed in this chapter, access protection involves both hardware and software. The hardware includes locks, keys, diskless PCs and biometrics. The software control access includes passwords and access restrictions to files and directories.

The communication protection to consider is call-back devices for verification and restricting dial-up capability.

Management controls and the user interface can not be overemphasized. The LAN manager is key to monitoring the system for security problems. A properly trained and educated user can eliminate many security problems.

Finally, the recovery system is an essential part of the design. Backups are required to avoid lost data, user mistakes and disaster recovery.

VI. RECOMMENDATIONS, CONCLUSIONS, AND SUGGESTIONS FOR FUTURE RESEARCH

A. SUMMARY OF RESULTS

The primary research question was to identify the security problems and control issues in local area networks (LANs). The aim of this thesis was to emphasize the prevention, detection and recovery elements as an integral part of LAN system design. A case study was designed to help officers stationed at naval patrol aviation squadrons gain an appreciation of the security issues in an unclassified network environment. Chapter III introduced the reader to basic LAN terminology including LAN architecture, topology and access procedures, and transmission media. Various security problems in LANs were discussed in detailed in Chapter IV. The primary issued related to hardware security resides in the fact that current systems lack built-in security mechanisms. Physical security has been a neglected area in implementing LANs. Effective measures should be taken to protect cabling, workstations and electrical power from unpredictable damage. As far as software is concerned, license violations, lack of robustness of PC-based operating systems, and viruses remain to be the most critical aspects. Also, illegal access by computer hackers presents a serious threat to remote connections. Finally, human-related security problems remain

the utmost issue to be addressed. Chapter V proposed a taxonomy of control solutions for LANs. Depending on the security spectrum, various physical, logical and administrative control measures could be devised. Password handling, recovery procedures including backups are amongst cost effective control strategies. It is not unusual to neglect LAN management as one aspect of LAN security. A management control plan should be carefully designed to appropriately empower the LAN's managers, and to promote users' awareness and involvement in a security program.

B. RECOMMENDED SOLUTIONS FOR THE PROPOSED CASE STUDY

The following security concerns are discussed in the case study:

- Diskette dilemma.
- Software theft/license violations.
- Access to computer bulletin boards.
- Physical access controls (locks).
- Password strategy.
- Viruses.
- The careless user.
- Electrical power.
- LAN manager controls.
- Recovery systems (backups, audit trails).
- Unauthorized access to information.
- Remote logins.

- Virus prevention.
- Tempest.

Although "Ringer's" recommendations are adequate, a few recommendations have flaws. For example, in the case, "Ringer" suggested incorrectly that the anti-virus program should be installed on the network. No software should be authorized on the network until tested on an isolated personal computer. Anti-virus programs although considered important in the prevention of viruses, when considered alone are inadequate. Management controls and the trained user are key elements in preventing viruses.

Another problem discussed by "Ringer" is password strategy. Password systems are doomed to fail if the codes are easy to remember.

LAN Manager was another topic of discussion in the case. As discussed in the thesis, a LAN of more than three computers require a LAN Manager. This job may be only collateral, but it is needed. The LAN Manager must monitor the network, check audit trails and set up backup procedures. Audit trails are important to read at least once a week but preferably once a day.

Tempest is for keeping RF signals contained. As discussed in the case, this has nothing to do with whether classified information can be installed on the network. Classified information should not be filed on the hard disk.

There is no optimal solution to designing a security system for a LAN. The level of security depends on the perceived threats and the risks. A risk assessment is required when changing the computer structure of an organization. After the risk assessment is completed, the security measures can be implemented.

Organizational objectives pertaining to security issues should be carefully weighted and prioritized. Finally, common sense is an important ingredient in designing a security system. Tight controls may reduce productivity and cause friction in the working environment. On the other hand, loose controls can result in security problems. A middle ground should be established.

C. SUGGESTIONS FOR FUTURE RESEARCH

There are at least two areas of study that could be suggested for future research.

First, all security program requires a risk assessment to identify and assess the exposures and their potential damages. The organization must determine the level of security perceived as necessary. A possible area for research is to incorporate risk assessment in the domain of LAN security along OPNAVINST 5239.1A guidelines.

Second, the materials discussed in this thesis should provide enough information to implement a decision support systems that would comply with the C2 level of security by

1992 in the Navy. The criteria classes of security are set from a level of class D for minimal protection to class A for the highest level of security. Class C2 involves discretionary access control, audit trails, and identification and authentication of users.

LIST OF REFERENCES

1. Chorafas, Dimitris N., Designing and Implementing Local Area Networks, McGraw-Hill Book Co., 1984.
2. Carr, Jim, "Take The Plunge: Networking 'On The Cheap'," Lan Magazine, July 1990.
3. Schneidewind, Norman F., "Principles of Local Area Networks," Encyclopedia of Science and Technology, McGraw-Hill Publishers, 1986.
4. Tanenbaum, Andrew S., Computer Networks, 2nd ed., Prentice-Hall Inc., 1988.
5. Leigh, W.E., and Burgess C., Distributed Intelligence. Trade-Offs and Decisions for Computer Information Systems, SouthWestern Publishing Co., 1987.
6. Watson, Richard, "Fortifying A LAN: Security On A LAN Means More Than Just Passwords," LAN Magazine, October 1988.
7. Madron, Thomas W., Local Area Networks: The Second Generation, John Wiley & Sons, Inc., 1988.
8. Stephenson, Peter. "Assessing Security: When is a LAN at Risk, and How Much Can a Company Lose?" LAN Magazine, February 1990.
9. Pfleeger, Charles P., Security in Computing, Prentice-Hall Inc., 1989.
10. Rosenthal, Robert, ed., "The Selection of Local Area Computer Networks," NBS Special Publication 500-96, 1982.
11. Katzan, H. Jr., Local Area Networks: A Manager's Guide, Carnegie Press, Inc., 1983.
12. National Computer Security Center. Personal Computer Security Considerations, 1985.
13. Brenner, Aaron, "The LAN Tutorial Series. Part 13: LAN Security," LAN Magazine, August 1989.
14. Mohanty, Munir, "Defending a LAN: The Tools and Tricks of Network Security," LAN Magazine, April 1988.

15. Keenan, Thomas P., "Emerging Vulnerabilities in Office Automation Security," Computer & Security, May 1989.
16. Coffee, Peter, "Virus Fears Cloud Other, More Likely Hazards," PC Week, 2 October 1989.
17. Ross, Steven J., "Viruses, Worms and Other (Computer) Plagues," The EDP Auditor Journal, Vol. 3, 1988.
18. Zajac, Bernard P. Jr., "Computer Viruses: Can They be Prevented?" Computer & Security, February 1990.
19. Highland, H.J., "Random Bits & Bytes," Computer & Security, December 1989.
20. Baker, Virginia E., "Infectious Diseases," LANTIMES, December 1989.
21. Jones, Laurie G., "Computer Viruses: Threat or Media Hype?" The EDP Auditor Journal, Vol. 3, 1988.
22. Nickson, James B., "Locking LANs: Detecting and Preventing the Malicious and Mischievous," LAN Magazine, October 1989.
23. Peters, A.J., "Essential Elements for the Development/Review of a PC Policy," The EDP Auditor Journal, Vol. 1, 1987.
24. Parker, Robert G., "Microcomputer Security and Control," The EDP Auditor Journal, Vol. 1, 1988.
25. Hertzoff, Ira, "How Fail-Safe is Your Local Area Network Security?" COMPUTERWORLD, 8 June 1987.
26. White, David W., "Entry-Level LANs: Seven Complete LANs for Under \$500," LAN Magazine, April 1989.
27. Severinsky, Alex J., "Sags and Surges: The Nature of Power Glitches--and How to Stop Them," LAN Magazine, March 1989.
28. Wood, Charles C., "Principles of Secure Information Systems Design," Computer & Security, February 1990.
29. Menkus, Belden, "Physical Security: Selecting an Access Control system," Computer & Security, May 1989.
30. Aarons, Richard, and Robin Raskin, "Security Strategies: Hardware Protection for PCs," PC Magazine, 28 April 1987.

31. Greenfield, David, "Sensible Paranoia: How to Protect the Treasures of the LAN," LAN Magazine, April 1989.
32. Nickson, Jay, and Don Leslie, "The Viral Threat: 'Vaccines' for the Smart LAN Manager," LAN Magazine, October 1988.
33. Greenfield, David, "For Your Eyes Only," LAN Magazine, April 1989.
34. Kneisel, Paul, "Picking Passwords: LAN Password Schemes that Work--and a Lot More that Don't," Lan Magazine, p. 42, May 1988.
35. Curry, David A., "Improving the Security of Your Unix System," SRI International, ITSTD-721-FR-90-21.
36. National Computer Security Center. Department of Defense Password Management Guideline, 1985.
37. Greeley, Kathy, "Backup Seen as Critical Issue for LANs," PC Week, 12 December 1988.
38. Brenner, Aaron, "The LAN Tutorial Series. Part 17: Backup," LAN Magazine, December 1989.
39. Schnaidt, Patricia, "Installation Insights: 20 Tips for Before, During and After," LAN Magazine, December 1987.
40. Marks, Howard, "No-Fault Insurance: Hardware and Software for Running Networks Continuously," LAN Magazine, July 1990.
41. Neff, Ken, "Fifteen Preventive Measures: Ways to Protect Your Network From Infection," LANTIMES, December 1989.
42. Stephenson, Peter, "J. Edgar's LAN: The FBI Uses a LAN to Help Keep America Safe," LAN Magazine, May 1989.
43. White, David W., "Cable Tips: Sound Advice from Cable Pros," LAN Magazine, November 1988.
44. Sampias, William J., and David J. Oberman, "Microcomputers: Where's the Security?" The EDP Auditor Journal, Vol. 3, 1987.
45. Sherizen, Sanford, "Make Security a Priority at Start of LAN Installation," COMPUTERWORLD, 27 June 1988.
46. Schmidt, Edwin A., "Security Methods Need Not Be Limiting," Government Computer News, 19 December 1988.

47. Humphrey, Watts S., Software Engineering and Design, Addison-Wesley Publishing Company, Inc., 1989.
48. Baskerville, Richard, Designing Information Systems Security, p. ix, John Wiley & Sons, Inc., 1988.

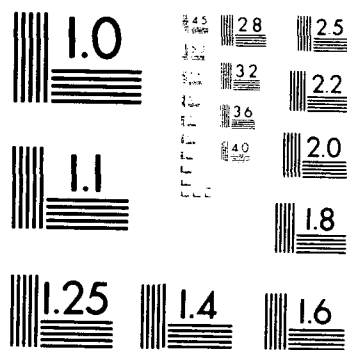
NO 4239 431

IDENTIFYING SECURITY PROBLEMS AND DEVISING CONTROL
SOLUTIONS IN A LOCAL AREA NETWORK: A CASE STUDY
APPROACH(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA
G J EVANS SEP 90 XN-NPS

UNCLASSIFIED

NL

END
FILMED
DTIC



MICROCOPY RESOLUTION TEST CHART
 NATIONAL BUREAU OF STANDARDS
 STANDARD REFERENCE MATERIAL 1010a
 (ANSI and ISO TEST CHART No. 2)

INITIAL DISTRIBUTION LIST

	No. Copies
1. Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2. Library, Code 52 Naval Postgraduate School Monterey, California 93943-5002	2
3. Curricular Officer, Code 37 Naval Postgraduate School Monterey, California 93943-5000	1
4. LCDR Gary J. Evans Patrol Squadron Nine (VP-9) FPO San Francisco, California 96601	2
5. Prof. Tung Bui, Code AS/Bd Naval Postgraduate School Monterey, California 93943-5000	3
6. Henry Smith Patrol Squadron Thirty-One (VP-31) Naval Air Station Moffett Field, California 93043	3